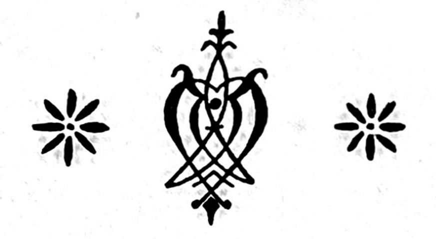
(Cours de Lemaire) Dany-Jack

I.M.S.P.
Université de Nice

Maitrise d'enseignement
(M 1)

U.V. ALGEBRE ET ARITHMETIQUE





Généralités sur les groupes

1 - Notion de groupe

- Rappels

1.1 - Définition : On appelle groupe tout ensemble G muni d'une loi de composition interne possédant les propriétés suivantes :

* cette loi est associative
* elle admet un élément neutre
* tout élément de G admet un symétrique

si de plus, la loi est commutative, le groupe est dit commutatif ou abélien.

• Ordre d'un groupe

1.2 - Définition : on appelle ordre d'un groupe G, son cardinal, c'est à dire le nombre de ses éléments.
Il existe des groupes d'ordre infini (ex : $\mathbb{Z}$, $\mathbb{R}$).

- Exemples de groupes

• L'ensemble des bijections d'un ensemble X sur lui-même, muni de la loi de composition des applications est un groupe ; ce groupe est appelé groupe symétrique de X et se note $\mathfrak{S}_X$
Si X est fini, de cardinal n ($n \geq 1$), le groupe symétrique de X est noté $\mathfrak{S}_n$ - Les éléments de $\mathfrak{S}_n$ sont appelés des permutations de X.

• L'ensemble des isométries(*) d'un espace métrique X, muni de la loi de composition des applications est un groupe qu'on note $Is(X, d)$ d étant la distance sur X.
$Is(X, d)$ est un sous-groupe de $\mathfrak{S}_X$.

(*) rappel : on appelle isométrie une bijection f d'un espace métrique E muni de la distance d sur un espace métrique E' muni de la distance d', telle que :

$$\forall x \in E,\ \forall y \in E \qquad d'(f(x), f(y)) = d(x, y)$$

• Groupes à n éléments

- $n = 1$

Le seul groupe à un élément est le groupe réduit à l'élément neutre

- $n = 2$

Soit $G = \{1, a\}$ où 1 est l'élément neutre, a un élément quelconque différent de 1

Par définition de l'élément neutre on doit avoir : $\begin{cases} 1.a = a \\ a.1 = a \\ 1.1 = 1 \end{cases}$

Pour que le groupe soit complètement défini il nous reste à connaître la valeur prise par $a^2 = a.a$.

En fait il y a 2 possibilités : soit $a^2 = 1$, soit $a^2 = a$

. $a^2 = a$ donne $a = 1$ ce qui est faux par hypothèse

. $a^2 = 1$ donne $a = a^{-1}$; donc dans le groupe à 2 éléments, a est son propre symétrique.

on obtient finalement, pour G, la table suivante :

·	1	a
1	1	a
a	a	1

On peut définir un isomorphisme entre $\mathbb{Z}/2\mathbb{Z}$ et $G = \{1, a\}$ de la manière suivante :

$$\mathbb{Z}/2\mathbb{Z} \longrightarrow \{1, a\} = G$$
$$\dot{0} \longrightarrow 1$$
$$\dot{1} \longrightarrow a$$

on en déduit que tout groupe à 2 éléments est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

- $n = p$, p premier

1.3. Proposition : Si G est un groupe à p éléments, avec p premier, alors il existe un isomorphisme entre $\mathbb{Z}/p\mathbb{Z}$ et G.

démonstration

Soit a un élément de G, $a \neq 1$.

Considérons l'homomorphisme de groupe :

$$f : \mathbb{Z} \ni n \longrightarrow a^n \in G$$

L'ensemble des puissances de a dans G est un sous-groupe de G

Pro 2 : G isomorphe à $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow$ G monogène d'ordre n

D'autre part, comme G possède p éléments, p premier, a^n est d'ordre 1 ou p (cf plus loin théorème 2.6) ;

a^n n'est pas d'ordre 1 car on a supposé par hypothèse $a \neq 1$ (si a^n était d'ordre 1 on aurait $a^n = 1$ donc $a = 1$)

Donc a^n est d'ordre p.

Autrement dit : $G = \text{Im } f$

On en déduit un homomorphisme surjectif :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ i & \longrightarrow & a^i \end{array}$$

et par passage au quotient (cf plus loin théorème 3.9) on obtient l'isomorphisme cherché :

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G \\ \dot{i} & \longrightarrow & a^i \end{array}$$

2 - Sous-groupes

- Rappels

2.1 - Définition : Soit H une partie non vide d'un groupe (G, .). On dit que H est un sous-groupe de G si :

- $a, b \in H \Rightarrow a.b \in H$
- $a \in H \Rightarrow a^{-1} \in H$

ces 2 conditions sont équivalentes à l'unique condition suivante :

$$a, b \in H \Rightarrow a.b^{-1} \in H$$

. Ordre d'un sous-groupe

2.2. Définition : On dit qu'un élément a d'un groupe G est d'ordre fini si le sous-groupe H de G engendré par a est fini. L'ordre de H est alors l'ordre de a.

- Sous-groupes distingués

2.3 - Définition : on dit qu'un sous-groupe H d'un groupe G est un sous-groupe distingué de G (et on note $H \triangleleft G$) si :

$$\forall x \in G, \quad \forall h \in H, \quad xhx^{-1} \in H$$

c'est à dire si, pour tout élément h de H le sous-groupe H contient aussi tous les éléments conjugués de h dans G.

• Soit H un sous-groupe de G ; on peut définir 2 relations d'équivalence sur G :

* une relation d'équivalence à droite qu'on note $\sim_H$:

$$x \sim_H y \iff x^{-1}y \in H \iff y \in xH \iff yH = xH$$

La classe à droite de x modulo H est xH ; on note l'ensemble quotient $G/\sim_H$ ou plus souvent G/H .

* une relation d'équivalence à gauche qu'on note ${}_H\sim$:

$$x \,{}_H\sim\, y \iff xy^{-1} \in H \iff x \in Hy \iff Hx = Hy$$

La classe à gauche de x modulo H est Hx ; on note l'ensemble quotient $G/{}_H\sim$ ou plus souvent $H\backslash G$.

En général : les deux relations d'équivalence sont différentes .

A partir de cette notion de classe d'équivalence on peut donner une nouvelle définition pour un sous-groupe distingué , équivalente à la première :

2.4 - Définition : on dit qu'un sous-groupe H d'un groupe G est distingué dans G si les classes à droite modulo H sont les classes à gauche modulo H c'est à dire : $\forall x \in G \quad xH = Hx$.

• Application

2.5 - Théorème de Lagrange : L'ordre de tout sous-groupe H d'un groupe G fini est un diviseur de l'ordre du groupe et :

$$\text{card}(G) = \text{card}(H) . [G:H]$$

($[G:H] = \text{card}(G/H)_d = \text{card}(G/H)_g$)

démonstration

Si H est un sous-groupe d'ordre k du groupe fini G d'ordre n , supposons qu'après avoir défini une relation d'équivalence à gauche , il existe j classes à gauche modulo H ; Toute classe à gauche xH contient exactement k éléments car si $xa_1 = xa_2$ avec $a_1, a_2 \in H$ alors $a_1 = a_2$

Par conséquent : $n = kj$

c'est l'égalité qu'on cherchait à obtenir .

• L'ordre d'un élément d'un groupe coïncidant avec l'ordre du sous-groupe qu'il engendre , il résulte du théorème de Lagrange que :

2.6 - Théorème : L'ordre de tout élément d'un groupe fini est un

diviseur de l'ordre du groupe considéré .

3 - Morphismes de groupes

- Homomorphismes

3.1 - Définition : Soient G et H deux groupes dont les lois sont notées respectivement $*$ et $\circ$. Un homomorphisme du groupe G dans le groupe H est une application f de G dans H telle que :

$$\forall (x,y) \in G^2 \qquad f(x * y) = f(x) \circ f(y)$$

si de plus l'application f est bijective , nous définissons un isomorphisme de groupe .

Exemples

- Si H est un sous-groupe distingué d'un groupe G ,

la surjection $\begin{array}{l} G \longrightarrow G/H \\ x \longrightarrow xH = \dot{x} \end{array}$ est un homomorphisme de groupe

dit homomorphisme canonique de G sur G/H .

- Soit G un groupe ;

L'application $\varphi : \begin{array}{l} G \longrightarrow \mathfrak{S}_G \\ g \longrightarrow (\forall h,\ h \rightarrow gh) \end{array}$ est un homomorphisme de groupe injectif.

c'est un homomorphisme car pour tout h :

$$\varphi(gg')(h) = (gg')(h) = g[g'(h)] = \varphi(g) \circ \varphi(g')(h)$$

il est injectif car si on considère 2 éléments g et g' de G :

$$\forall h \ , \ gh = g'h \quad \Rightarrow \quad g = g'$$

- Automorphismes intérieurs

3.2 - Définition : Soient G un groupe et x un élément de G .
L'application $\sigma_x : \begin{array}{l} G \longrightarrow G \\ y \longrightarrow xyx^{-1} \end{array}$ est un automorphisme de G
dit automorphisme intérieur de G .

L'ensemble des automorphismes intérieurs de G, noté Int(G) , est un sous-groupe du groupe des automorphismes de G , Aut(G)

Vérifions que l'application définie par $\forall y \in G \quad \sigma_x(y) = xyx^{-1}$ est bien un automorphisme de G :

- c'est une bijection ; on le montre directement en mettant en évidence une application réciproque :

$\forall z \in G$, $\exists!\, y$ tq : $xyx^{-1} = z$; on a $y = x^{-1}zx$

Donc : $(\sigma_x)^{-1} = \sigma_{x^{-1}}$

- c'est un homomorphisme ; en effet :

$\forall y \in G$, $\forall z \in G$ $\sigma_x(y) \cdot \sigma_x(z) = xyx^{-1}xzx^{-1} = xyzx^{-1} = \sigma_x(yz)$

. Remarque : un groupe commutatif n'a pas d'automorphismes intérieurs non triviaux (ie autres que l'identité).

. Autre remarque : D'après la définition 2.3 un sous groupe est distingué si et seulement si il est invariant par tout automorphisme intérieur.

3.3. Proposition : L'application $\alpha : \begin{array}{l} G \to \mathrm{Aut}(G) \\ x \to \sigma_x \end{array}$ est un homomorphisme de groupe.

démonstration

$\forall x, x' \in G$ $\alpha(xx')(y) = \sigma_{xx'}(y) = xx'.y.(xx')^{-1}$

$= x\,(x'yx'^{-1})\,x^{-1}$

$= x\ \sigma_{x'}(y)\ x^{-1}$

$= \sigma_x \circ \sigma_{x'}(y)$

$= \alpha(x).\alpha(x')\,(y)$

. Remarque : En général cet homomorphisme α n'est pas surjectif son image est $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$.

. Centre d'un groupe

3-4. Définition : Le noyau de l'application $\alpha : G \to \mathrm{Aut}(G)$ est appelé centre du groupe G et se note $Z(G)$.

3.5 - Proposition : Le centre est l'ensemble des éléments qui commutent avec tous les autres éléments du groupe

ie : $Z(G) = \{x \in G \ /\ \forall y \in G \quad yx = xy\}$

En effet $x \in \mathrm{Ker}\,\alpha \iff \sigma_x = id \iff \forall y \quad xyx^{-1} = y$

$\iff \forall y \quad xy = yx$

Remarque : Il existe des groupes dont le centre est réduit à l'élément neutre ; Mais si un groupe est abélien son centre, c'est lui-même.

3.6. Proposition : Le noyau de tout homomorphisme φ d'un groupe G sur un autre groupe G' est un sous-groupe distingué de G.

démonstration

soit donc $\varphi : G \longrightarrow G'$

. commençons par montrer que $\ker \varphi$ est un sous-groupe de G

si $a \in \ker\varphi$ et $b \in \ker\varphi$ alors $\varphi(a) = \varphi(b) = 1_{G'}$

et par suite comme φ est un homomorphisme $\varphi(ab) = \varphi(a).\varphi(b) = 1_{G'}$

donc $ab \in \ker\varphi$.

Par ailleurs si $a \in \ker\varphi$ c'est à dire si on a $\varphi(a) = 1_{G'}$

alors $\varphi(a^{-1}) = [\varphi(a)]^{-1} = 1_{G'}^{-1} = 1_{G'}$ soit $a^{-1} \in \ker\varphi$

. soit enfin $a \in \ker\varphi$ ie $\varphi(a) = 1_{G'}$

alors $\forall x \in G$ $\varphi(x^{-1}ax) = \varphi(x^{-1}).\varphi(a).\varphi(x) = (\varphi(x))^{-1}1_{G'}\varphi(x) = 1_{G'}$

Ainsi $\ker\varphi$ est un sous-groupe de G tel qu'avec tout élément a ce sous-groupe contient tous les éléments conjugués de a ;

Par conséquent le sous-groupe $\ker\varphi$ est distingué dans G.

3.7. Conséquence : Le centre $Z(G)$ d'un groupe G est un sous-groupe distingué de G.

. On a vu que $\mathrm{Int}(G)$ était un sous-groupe de $\mathrm{Aut}(G)$; En fait :

3.8. Proposition : $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$

démonstration

soit $\sigma_x \in \mathrm{Int}(G)$ alors on vérifie immédiatement que :

$\forall \tau \in \mathrm{Aut}(G)$ $\tau \circ \sigma_x \circ \tau^{-1} = \sigma_{\tau(x)}$

et ceci montre que $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.

- Décomposition canonique d'un homomorphisme

3.9. Théorème : Pour tout homomorphisme φ d'un groupe G dans un groupe G' il existe :

- un homomorphisme surjectif $\pi : G \longrightarrow G/\ker\varphi$
- un homomorphisme injectif $i : \mathrm{Im}\varphi \longrightarrow G'$
- un isomorphisme $\bar{\varphi} : G/\ker\varphi \longrightarrow \mathrm{Im}\varphi$

tels que : $\varphi = i \circ \bar{\varphi} \circ \pi$ (cette décomposition est unique)

on peut traduire ce résultat dans le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & & \uparrow i \\ G/\mathrm{Ker}\,\varphi & \xrightarrow[\overline{\varphi}]{} & \mathrm{Im}\,\varphi \end{array}$$

démonstration du théorème

on prend pour i l'injection canonique $\mathrm{Im}\,\varphi \to G'$

pour π la surjection canonique $G \to G/\mathrm{Ker}\,\varphi$ (on a vu que $\mathrm{Ker}\,\varphi$ était un sous-groupe distingué de G)

montrons qu'il existe un isomorphisme entre $G/\mathrm{Ker}\,\varphi$ et $\mathrm{Im}\,\varphi$

considérons l'application $\overline{\varphi}$: $G/\mathrm{Ker}\,\varphi \longrightarrow \mathrm{Im}\,\varphi$

$\dot{x} \longrightarrow \varphi(x)$

c'est un homomorphisme car :

$\forall\, \dot{x}, \dot{y} \in G/\mathrm{Ker}\,\varphi \qquad \overline{\varphi}(\dot{x}\,\dot{y}) = \overline{\varphi}(\dot{\overline{xy}}) = \varphi(xy) = \varphi(x).\varphi(y) = \overline{\varphi}(\dot{x}).\overline{\varphi}(\dot{y})$

il est injectif car :

$\dot{x} = \dot{y}$ dans $G/\mathrm{Ker}\,\varphi \Leftrightarrow x^{-1}y \in \mathrm{Ker}\,\varphi \Leftrightarrow \varphi(x^{-1}y) = 1_{G'} \Leftrightarrow \varphi(x) = \varphi(y)$

il est évidemment surjectif.

Donc on a bien un isomorphisme entre $G/\mathrm{Ker}\,\varphi$ et $\mathrm{Im}\,\varphi$.

- Application au cas des automorphismes

on a vu que l'application $G \xrightarrow{\alpha} \mathrm{Aut}(G)$ est un homomorphisme de groupe (proposition 3.3) ; Alors d'après le théorème 3.9 on déduit une factorisation de α suivant le diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & \mathrm{Aut}(G) \\ \pi \downarrow & & \uparrow i \\ G/Z(G) & \xrightarrow[\overline{\alpha}]{} & \mathrm{Int}(G) \end{array}$$

En particulier on voit que $G/Z(G)$ est isomorphe à $\mathrm{Int}(G)$.] intéressant

4 - Actions de groupes

- Définitions

> 4.1 - Définition : Soient G un groupe et X un ensemble ; on dit que G opère à gauche sur X si on s'est donné une application φ :
>
> $\varphi : G \times X \longrightarrow X$
>
> $(g, x) \longrightarrow \varphi(g,x) = g.x$
>
> vérifiant les conditions suivantes :
>
> $\forall g\ \forall g' \in G,\ \forall x \in X \qquad g(g'.x) = gg'.x$
>
> $\forall x \in X \qquad 1_G.x = x$

Dans les mêmes conditions on dit que G opère à droite sur X si on s'est donné une application φ :

$$\varphi : X \times G \longrightarrow X$$
$$(x,g) \longrightarrow \varphi(x,g) = x.g$$

vérifiant les conditions suivantes :

$$\forall g \ \forall g' \in G \ , \forall x \in X \qquad (x.g)g' = x.(gg')$$
$$. \ \forall x \in X \qquad x.1_G = x$$

- Exemple : on peut faire opérer un groupe G sur lui-même :
  - à gauche, par translation à gauche
    à l'aide de l'application : $(g,g') \longrightarrow g.g'$
  - à droite, par translation à droite
    à l'aide de l'application : $(g,g') \longrightarrow g'.g$
  - à gauche, par conjugaison
    à l'aide de l'application : $(g,g') \longrightarrow g.g'.g^{-1}$

- Orbites

4.2. Définition : Soit G un groupe opérant sur un ensemble X et soit $x \in X$ on appelle orbite de x sous G l'ensemble noté $G.x$ des éléments de X de la forme $g.x$ où $g \in G$:

$$G.x = \{ y \in X \ \text{tq} \ \exists g \in G : g.x = y \}$$

- Considérons la relation entre éléments de X définie de la manière suivante : $x \sim_G y \iff \exists g \in G \ \text{tq} \ y = g.x$

c'est une relation d'équivalence sur X

en effet : . elle est reflexive : $x \sim_G x$

il suffit de prendre $g = 1_G$ alors $x = 1_G.x$

. elle est symétrique : $x \sim_G y \Rightarrow y \sim_G x$

car $g.x = y \Rightarrow x = g^{-1}.y$ (g est un homomorphisme)

. elle est transitive : $x \sim_G y$ et $y \sim_G z \Rightarrow x \sim_G z$

car si $g.x = y$ et $g'.y = z$ alors $z = g'(g.x) = g'g.x$

Alors la classe d'équivalence (pour cette relation) d'un élément x de X est l'orbite de x d'après la définition 4.2 .

L'ensemble des orbites de X sous G forme une partition de X .

- Stabilisateur

4.3 - Définition : Soit G un groupe opérant sur un ensemble X. Pour chaque élément x de X, les $g \in G$ tels que $g.x = x$ forment un sous-groupe de G ; on l'appelle le stabilisateur de x dans G (ou encore le groupe d'isotropie de x) et on le note G_x.

$$G_x = \{ g \in G \;/\; g.x = x \}$$

. Remarque : en général G_x n'est pas distingué dans G

4.4 - Définition : Soient H et H' deux sous-groupe d'un groupe G ; on dit que H et H' sont conjugués dans G s'il existe un automorphisme intérieur φ_a tel que $H' = \varphi_a(H) = aHa^{-1}$.

4.5 - Proposition : Deux stabilisateurs G_x et G_y dans G sont conjugués si les points x et y sont dans la même orbite.

démonstration

soient x et y 2 points d'une même orbite : $y = g_0.x$

comparons G_x et G_y

$g \in G_x \iff g.x = x$ or $x = g_0^{-1}y$ donc :

$g.g_0^{-1}y = g_0^{-1}y \iff g_0 g g_0^{-1} y = y \iff g_0 g g_0^{-1} \in G_y$

on en déduit : $G_y = g_0 G_x g_0^{-1}$

Autrement dit G_x et G_y sont conjugués -

5 - Etude des groupes symétriques

- Rappels

5.1 - Définition : Le groupe symétrique à n variables noté $\mathfrak{S}_n$ est le groupe des permutations de n objets.

. Rappelons que dans le 1er paragraphe de ce chapitre nous avons vu que l'ensemble $\mathfrak{S}(X)$ des bijections d'un ensemble X sur lui-même est un groupe appelé groupe symétrique ; lorsque X est fini formé des entiers $1, 2, \ldots n$ $(X = \{1, 2, \ldots n\})$ le groupe symétrique de X est noté $\mathfrak{S}_n$, ses éléments étant alors appelés permutations de X.

. Remarque : l'ensemble des éléments de $\mathfrak{S}_n$ qui laissent fixe n s'identifie à $\mathfrak{S}_{n-1}$.

conséquence :

5.2 - Proposition : Le groupe symétrique $\mathfrak{S}_n$ est un groupe à $n!$ éléments ie :

$$\# \mathfrak{S}_n = n!$$

démonstration

Nous allons montrer cette proposition par recurrence sur n

. pour $n = 1$ il est évident que : $\# \mathfrak{S}_1 = 1$

(nombre de permutation d'un ensemble à 1 élément $= 1!$)

. hypothèse de récurrence : $\# \mathfrak{S}_{n-1} = (n-1)!$

. montrons que la proposition est alors vraie pour n

nous venons de voir que l'on pouvait considerer $\mathfrak{S}_{n-1}$ comme un sous groupe de $\mathfrak{S}_n$. D'après le théorème 2.5 on a :

$$\# \mathfrak{S}_n = \# (\mathfrak{S}_n / \mathfrak{S}_{n-1}) \cdot \# \mathfrak{S}_{n-1}$$

comme par hypothèse de récurrence $\# \mathfrak{S}_{n-1} = (n-1)!$, il nous suffit de prouver qu'on a exactement n classes modulo $\mathfrak{S}_{n-1}$ dans $\mathfrak{S}_n$.

Pour cela considérons l'application :

$$f : \mathfrak{S}_n \longrightarrow X = \{1, 2, \dots n\}$$
$$\sigma \longrightarrow f(\sigma) = \sigma(n)$$

cette application est surjective.

D'autre part si σ et σ' sont 2 permutations de $X = \{1, 2 \dots n\}$ alors : $f(\sigma) = f(\sigma') \Leftrightarrow \sigma(n) = \sigma'(n) \Leftrightarrow n = \sigma^{-1} \cdot \sigma'(n)$

autrement dit : $f(\sigma) = f(\sigma') \Leftrightarrow \sigma^{-1} \cdot \sigma' \in \mathfrak{S}_{n-1}$

on en déduit donc l'existence d'une bijection φ :

$$\varphi : (\mathfrak{S}_n / \mathfrak{S}_{n-1}) \longrightarrow X = \{1, 2, \dots n\}$$

d'où $\# (\mathfrak{S}_n / \mathfrak{S}_{n-1}) = \# X = n$

- Eléments particuliers de $\mathfrak{S}_n$

1 - Les transpositions

5.3 - Définition : Dans le groupe $\mathfrak{S}_n$, on dit qu'une permutation t est une transposition s'il existe i et j dans $\{1, 2 \dots n\}$ tels que :

- $t(i) = j$; $t(j) = i$
- $t(k) = k \quad \forall k \in \{1, 2, \dots n\} \setminus \{i, j\}$

(on suppose $n \geqslant 2$) - on note cette transposition (i, j).

. Propriété : pour toute transposition t, on a $t^2 = id$ et donc $t^{-1} = t$

> **5.4 - Proposition :** Pour $n \geq 2$, le groupe $\mathfrak{S}_n$ est engendré par les transpositions qu'il contient.

démonstration

Nous allons montrer que toute permutation $\sigma \in \mathfrak{S}_n$ peut s'écrire comme un produit de transpositions.

Pour cela raisonnons par récurrence sur n :

. pour $n = 2$ la proposition est triviale ;

. supposons la vraie au rang $(n-1)$; c'est à dire tout élément de $\mathfrak{S}_{n-1}$ peut s'écrire comme un produit de transpositions t_i

. Soit $\sigma \in \mathfrak{S}_n$

Posons $k = \sigma(n)$ et considérons $\tau = (k, n) \circ \sigma$

Il est clair que : $\tau(n) = n$

τ laisse fixe n ; elle appartient donc à $\mathfrak{S}_{n-1}$; alors d'après l'hypothèse de recurrence on peut écrire :

$$\tau = t_1 \circ \dots \circ t_r \quad \text{où les } t_j \text{ sont des transpositions}$$

Et par suite :

$$\sigma = (k, n) \circ t_1 \circ \dots \circ t_r \qquad \left((k,n)^{-1} = (k,n) \right)$$

on a ainsi pu écrire σ sous forme d'un produit de transpositions.

2. Les cycles

5.5 - Définition : Dans le groupe $\mathfrak{S}_n$, on appelle cycle une permutation γ telle qu'il existe une suite d'entiers $i_1, i_2, \dots, i_\ell$, 2 à 2 distincts tels que :
- $\gamma(i_1) = i_2$, ..., $\gamma(i_{\ell-1}) = i_\ell$, $\gamma(i_\ell) = i_1$
- $\gamma(k) = k$ si $k \in \{1, 2 \dots n\} \setminus \{i_1, \dots i_\ell\}$

ℓ est alors la longueur du cycle

De plus on a : $\gamma^\ell = id$

> **5.6 - Théorème :** Pour toute permutation σ de $\mathfrak{S}_n$, il existe un ensemble de cycles $\gamma_1, \dots, \gamma_n$ disjoints tel que :
> $$\sigma = \prod_i \gamma_i$$

démonstration

. remarque préliminaire : si 2 cycles γ' et γ'' sont disjoints alors $\gamma' \gamma'' = \gamma'' \gamma'$

. Soit donc $\sigma \in \mathfrak{S}_n$; considérons le sous-groupe de $\mathfrak{S}_n$ engendré par σ :

$$\Gamma = \{\sigma^n, n \in \mathbb{Z}\} = \{1, \sigma, \dots \sigma^m\} \quad (\text{avec } \operatorname{ord}(\sigma) = m+1)$$

Le groupe Γ opère sur l'ensemble $\{1, 2, \dots n\}$; cet ensemble admet donc une partition en orbites $I_1, \dots, I_\ell$

Avec les notations conventionnelles on a :

$$I_1 = \Gamma . a_1 \quad , I_2 = \Gamma . a_2 \quad , \quad \dots . \quad I_\ell = \Gamma . a_\ell$$

où : $\quad I_j = \{a_j, \sigma(a_j), \dots, \sigma^{\ell_j}(a_j)\}$ et ℓ_j / m

considérons alors la permutation :

$$\begin{cases} \gamma_j(i) = \sigma(i) & \text{si } i \in I_j \\ \gamma_j(i) = i & \text{si } i \notin I_j \end{cases}$$

on vérifie facilement que :

- γ_j est un cycle de longueur ℓ_j
- $\prod_j \gamma_j = \sigma$

5.7 - Proposition : Deux permutations σ et σ' de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles admettent des décompositions en cycles disjoints de mêmes longueurs.

démonstration

($\Rightarrow$) on suppose que σ et σ' sont 2 permutations conjuguées autrement dit $\exists\, h \in \mathfrak{S}_n$ tq $\sigma' = h \sigma h^{-1}$

soit une décomposition de σ en cycles disjoints :

$$\sigma = \prod_{i=1}^{\ell} \gamma_i$$

Alors $\quad \sigma' = h \sigma h^{-1} = h . \prod_i^{\ell} \gamma_i . h^{-1} = \prod_{i=1}^{\ell} h . \gamma_i h^{-1}$

il est facile de voir que les $h.\gamma_i h^{-1}$ sont des cycles disjoints on obtient ainsi une décomposition de σ' en cycles disjoints de mêmes longueurs que ceux de la décomposition de σ.

($\Leftarrow$) considérons les décompositions de σ et σ' en cycles disjoints de mêmes longueurs :

$$\sigma = (a_1, \sigma(a_1) \dots \sigma^{k_1}(a_1))(a_2, \sigma(a_2) \dots \sigma^{k_2}(a_2)) \dots$$
$$= \quad \gamma_1 \quad . \quad \gamma_2 \quad \dots$$

$$\sigma' = (b_1, \sigma'(b_1) \dots \sigma'^{k_1}(b_1))(b_2, \sigma'(b_2) \dots \sigma'^{k_2}(b_2)) \dots$$
$$= \quad \gamma'_1 \quad . \quad \gamma'_2 \quad \dots$$

Soit h l'application définie par :

$$\begin{cases} a_i \longrightarrow b_i \\ \sigma(a_i) \longrightarrow \sigma'(b_i) \\ - - - - - - - - - \\ \sigma^{\ell}(a_i) \longrightarrow \sigma'^{\ell}(b_i) \qquad \ell \leq k_i \end{cases}$$

on vérifie alors aisément que : $h \cdot \sigma = \sigma' \cdot h$

il suffit de le vérifier sur un élément, on a :

$$h \cdot \sigma(a_1) = \sigma'(b_1) = \sigma' \cdot h(a_1)$$

de même $\quad h \cdot \sigma(\sigma^{\ell}(a_1)) = h\,\sigma^{\ell+1}(a_1) = \sigma'^{\ell+1}(b_1) = \sigma' \cdot h(\sigma^{\ell}(a_1))$

• Application : soit H un sous-groupe distingué de $\mathfrak{S}_n$; si H contient une transposition alors H contient aussi toutes les autres transpositions et $H = \mathfrak{S}_n$.

En effet si $H \triangleleft \mathfrak{S}_n$, $\forall h \in H$, $\forall \sigma \in \mathfrak{S}_n$ $\quad \sigma h \sigma^{-1} \in H$

ie un sous-groupe distingué contient tous les conjugués de ses éléments (cf définition 2.3)

Or d'après la proposition 5.7 toutes les transpositions sont conjuguées

D'autre part d'après la proposition 5.4 les transpositions engendrent $\mathfrak{S}_n$ donc $H = \mathfrak{S}_n$.

- Signature d'une permutation

5.8 - Définition : on appelle signature d'une permutation l'application :

$$\varepsilon : \mathfrak{S}_n \longrightarrow \{-1, +1\}$$

définie par : $$\varepsilon(\sigma) = \frac{\prod_{i<j} (\sigma(j) - \sigma(i))}{\prod_{i<j} (j - i)}$$

on vérifie que : - ε est un homomorphisme de groupe

- la signature d'une transposition quelconque est -1.

5.9 - Définition : Le noyau de l'homomorphisme ε s'appelle le <u>groupe alterné</u> ; on le note $\mathfrak{A}_n$; c'est un sous-groupe distingué de $\mathfrak{S}_n$; c'est l'ensemble des permutations qui sont égales à un produit d'un nombre pair de transpositions.

• On démontre que si $n \neq 4$ le groupe $\mathfrak{S}_n$ n'a pas d'autres sous-groupes distingués non triviaux que $\mathfrak{A}_n$.

. Pour $n = 4$

le groupe $K = \{ (1,2)(3,4) , (1,3)(2,4) ,$

$(1,4)(2,3) , (1)(2)(3)(4) = id \}$

est distingué dans $\mathfrak{A}_4$ et dans $\mathfrak{S}_4$

c'est un groupe à 4 éléments appelé groupe de Klein .

$\mathbb{Z}$

1 - Définition - Structure

- rappels sur $\mathbb{N}$

$\mathbb{N}$ est en général défini à partir des axiomes de Péano ; mais on ne peut pas démontrer que ces axiomes sont non-contradictoires (Gödel).

S'il y a une contradiction en mathématique, elle vient de $\mathbb{N}$!

- définition de $\mathbb{Z}$

$\mathbb{Z}$ est construit par symétrisation de $\mathbb{N}$.

$\mathbb{Z}$ est l'ensemble des entiers rationnels.

- structure de $\mathbb{Z}$

$(\mathbb{Z},+)$ est un groupe commutatif.

$\mathbb{Z}$ est engendré par un élément : 1 (il est aussi engendré par -1)

$(\mathbb{Z},+,.)$ est un anneau commutatif unitaire.

2. Sous-groupes de $\mathbb{Z}$

- définition - propriétés

2.1 - Théorème : L'ensemble des sous-groupes de $\mathbb{Z}$ est l'ensemble $\{n\mathbb{Z}, n \in \mathbb{N}\}$.

La démonstration utilise le fait qu'il existe une division euclidienne dans $\mathbb{Z}$.

Soit $H \subset \mathbb{Z}$; on veut montrer que H est de la forme $n\mathbb{Z}$ $(H \neq \{0\})$

(La réciproque est évidente : $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$)

Soit $n = \inf\{H \cap \mathbb{N}^*\}$

$\forall a \in H$ montrons que n divise a ; pour ce faire écrivons la division euclidienne de a par n :

$\forall a \ \forall n \ \exists! q \ \exists! r$ tels que : $a = nq + r$ et $0 \leq r < n$

on en tire $r = a - nq$; $a \in H$, $nq \in H$ donc $r \in H$

or $0 \leq r < n$, comme n est le plus petit élément positif de H on en déduit que $r = 0$; d'où $a = nq$ ce qui montre que n divise a.

En définitive $\forall a \in H$ a s'écrit sous la forme nq, $n \in \mathbb{N}$, $q \in \mathbb{Z}$

Donc H est bien de la forme $n\mathbb{Z}$.

- Soit $\mathcal{T}$ l'ensemble des sous-groupes de $\mathbb{Z}$

On vient de voir que l'application $\begin{matrix} \mathcal{T} \to \mathbb{N} \\ n\mathbb{Z} \to n \end{matrix}$ est une bijection

Si on considère sur $\mathcal{T}$ la relation d'ordre "inclusion" alors il existe sur $\mathbb{N}$ une relation d'ordre correspondante :

$$\boxed{n\mathbb{Z} \subset m\mathbb{Z} \iff m \text{ divise } n}$$

On définit ainsi sur $\mathcal{T}$ un treillis (ensemble totalement ordonné où tout couple d'éléments admet un sup. et un inf.)

$$\sup(n\mathbb{Z}, m\mathbb{Z}) = n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z} \quad \text{où } d = \text{pgcd}(m,n)$$

$$\inf(n\mathbb{Z}, m\mathbb{Z}) = n\mathbb{Z} \cap m\mathbb{Z} = \mu\mathbb{Z} \quad \text{où } \mu = \text{ppcm}(m,n)$$

2.2 - Théorème : Soient $a\mathbb{Z}$ et $b\mathbb{Z}$ deux sous-groupes de $\mathbb{Z}$:

si $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et $\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$

alors $ab\mathbb{Z} = \mu d\mathbb{Z}$

La démonstration se fait en deux étapes :

- on commence par montrer que $ab\mathbb{Z} \supset \mu d\mathbb{Z}$

par hypothèse $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

on en déduit : $\mu d\mathbb{Z} = \mu(a\mathbb{Z} + b\mathbb{Z}) = \mu a\mathbb{Z} + \mu b\mathbb{Z}$

d'où $\mu d\mathbb{Z} = a\mu\mathbb{Z} + b\mu\mathbb{Z}$

or $\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ $\quad \mu d\mathbb{Z} = a(a\mathbb{Z} \cap b\mathbb{Z}) + b(a\mathbb{Z} \cap b\mathbb{Z})$

$\mu d\mathbb{Z} = a^2\mathbb{Z} \cap ab\mathbb{Z} + ba\mathbb{Z} \cap b^2\mathbb{Z}$

mais $a^2 \cap ab\mathbb{Z} \subset ab\mathbb{Z}$ et $ba\mathbb{Z} \cap b^2\mathbb{Z} \subset ab\mathbb{Z}$

donc $\mu d\mathbb{Z} \subset ab\mathbb{Z}$

- on montre maintenant que : $ab\mathbb{Z} \subset \mu d\mathbb{Z}$

on a $\mu d\mathbb{Z} = d\mu\mathbb{Z} = d(a\mathbb{Z} \cap b\mathbb{Z})$

$= da\mathbb{Z} \cap db\mathbb{Z}$

$= a(a\mathbb{Z} + b\mathbb{Z}) \cap b(a\mathbb{Z} + b\mathbb{Z})$

$= (a^2\mathbb{Z} + ab\mathbb{Z}) \cap (ba\mathbb{Z} + b^2\mathbb{Z})$

on voit que : $ab\mathbb{Z} \subset (a^2\mathbb{Z} + ab\mathbb{Z}) \cap (ba\mathbb{Z} + b^2\mathbb{Z})$

donc $ab\mathbb{Z} \subset \mu d\mathbb{Z}$

Finalement on a bien l'égalité.

2.3. Définition (Bezout) : on dit que 2 nombres a et b sont premiers entre eux si : $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

2.4. Théorème de Gauss : $a, b, c \in \mathbb{Z}$; $\begin{cases} a / bc \\ (a,b) = 1 \end{cases} \Rightarrow a / c$

démonstration

$a / bc \iff bc\mathbb{Z} \subset a\mathbb{Z}$

$(a, b) = 1 \Rightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} \Rightarrow ac\mathbb{Z} + bc\mathbb{Z} = c\mathbb{Z}$

on vient de voir que (par hypothèse) $bc\mathbb{Z} \subset a\mathbb{Z}$

d'autre part on a : $ac\mathbb{Z} = c(a\mathbb{Z}) \subset a\mathbb{Z}$

on en déduit donc que : $ac\mathbb{Z} + bc\mathbb{Z} \subset a\mathbb{Z}$

c'est à dire : $c\mathbb{Z} \subset a\mathbb{Z}$

or $c\mathbb{Z} \subset a\mathbb{Z} \iff a / c$

- Sous-groupes maximaux - Nombres premiers

Rappel : un élément d'un ensemble ordonné est maximal s'il n'admet pas de majorant strict (ie il n'admet pas d'éléments strictement plus grands que lui ; mais attention il peut y avoir des éléments qui ne sont pas comparables avec lui)

On cherche les sous-groupes maximaux dans $\mathcal{M} - \{\mathbb{Z}\}$ ($\mathcal{M}$ étant l'ensemble des sous-groupes de $\mathbb{Z}$)

On rappelle que p est premier s'il n'admet comme seuls diviseurs que 1 et lui-même ; d'où on déduit :

2.5. Proposition : $p\mathbb{Z}$ est un sous-groupe maximal si et seulement si p est premier.

2.6. Théorème : Tout sous groupe de $\mathbb{Z}$ est contenu dans un sous-groupe maximal (i.e tout nombre entier possède un diviseur premier).

démonstration par l'absurde

Soit H un sous-groupe de $\mathbb{Z}$ qui n'est contenu dans aucun sous-groupe maximal

H étant non maximal, il existe $H_1 \supsetneq H$

de même H_1 étant non maximal, il existe $H_2 \supsetneq H_1$

etc ...

on en déduit l'existence d'une suite infinie H_n telle que $H_n \subsetneq H_{n+1}$

on pose $H_\infty = \bigcup_{n \in \mathbb{N}} H_n$

H_∞ est de la forme $r\mathbb{Z}$ car H_∞ est encore un sous-groupe de $\mathbb{Z}$

$r \in H_\infty$ et en particulier $\exists n$ tel que $r \in H_n$ puisque $H_\infty = \bigcup_n H_n$

on en déduit que : $r\mathbb{Z} \subset H_n$

et comme d'autre part $H_n \subset r\mathbb{Z}$

on a : $r\mathbb{Z} = H_n = H_\infty$

ceci contredit le fait qu'on puisse construire une suite strictement croissante de sous-groupes.

Cette démonstration a montré en outre que toute suite croissante de sous-groupes de $\mathbb{Z}$ est stationnaire.

. conséquence

2.7. Théorème d'Euclide : il y a un nombre infini de nombres premiers.

démonstration par l'absurde

Soit $\mathbb{P}$ l'ensemble des nombres premiers

Supposons que $\mathbb{P}$ est fini $\mathbb{P} = \{p_1, p_2, \dots p_k\}$

Soit $n = \left(\prod_{i=1}^{k} p_i\right) + 1$; ce nombre n'est pas divisible par un p_i $1 \leq i \leq k$ et pourtant d'après le théorème précédent il admet certainement un diviseur premier p

donc $\exists p$, $p \notin \{p_1 \dots p_k\}$, p premier

ceci contredit l'hypothèse à savoir que tous les nombres premiers sont les $p_1 \dots p_k$

3 - Quotients de $\mathbb{Z}$

- Idéal

3.1. Définition : soit $(A,+,.)$ un anneau commutatif et I un sous-groupe de $(A,+)$.

I est un idéal de A si : $\forall a \in A$, $\forall x \in I$ $ax \in I$

ou encore si : $A.I \subset I$

. remarque : si l'anneau n'est pas commutatif on distingue idéaux à droite et idéaux à gauche.

- Tout sous-groupe de $\mathbb{Z}$ est un idéal de $\mathbb{Z}$

- Anneau quotient

Soit $(A, +, .)$ un anneau commutatif

Soit I un sous-groupe du groupe additif $(A, +)$

L'application $\pi : A \longrightarrow A/I$ est un homomorphisme de groupes

La question qu'on se pose est de savoir s'il existe une structure d'anneau sur A/I telle π soit un homomorphisme d'anneaux

. On peut déjà dire que s'il existe une telle structure sur A/I elle est <u>unique</u> :

$$\pi(a) . \pi(b) = \pi(ab)$$

. Remarque : s'il existe une loi sur A/I telle que π soit un homomorphisme d'anneaux on dit que cette loi est la loi quotient.

3.2 . Proposition : Il existe une structure d'anneau sur A/I telle que π soit un homomorphisme d'anneaux si et seulement si I est un idéal de A.

démonstration

- Supposons que A/I possède une structure d'anneau

on a : $I = \pi^{-1}(\dot{0})$

Montrons que I est un idéal

$a \in A$, $x \in I$ $\quad \pi(ax) = \pi(a).\pi(x) = 0$ car $x \in I \Rightarrow \pi(x) = 0$

donc $ax \in I$

- Soit I un idéal de A

il faut montrer que A/I est un anneau

Etant donnés $\pi(a)$ et $\pi(b)$ dans A/I il faut montrer que $\pi(a.b)$ ne dépend que de $\pi(a)$ et $\pi(b)$

Soient $a', b' \in A$ tels que $\pi(a) = \pi(a')$ et $\pi = \pi(b')$

$$\pi(a'-a) = 0 \quad \text{d'où} \quad x = a - a' \in I$$
$$\pi(b'-b) = 0 \quad \text{d'où} \quad y = b - b' \in I$$

On a : $\pi(a'b') = \pi((a+x)(b+y)) = \pi(ab + xb + ay + xy) = \pi(ab)$

car $xb + ay + xy \in I$

remarque : on ne peut faire le quotient d'un anneau non commutatif que par un idéal bilatère (ie. un idéal à droite et à gauche)

- Quotients de $\mathbb{Z}$: ce sont les $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est un anneau ; il est appelé anneau des congruences modulo n (n est quelconque)

Soient 2 nombres a et b, soient α et β leur reste modulo n

on a : $\begin{cases} a = nq + \alpha \\ b = nr + \beta \end{cases}$ ce qui s'écrit aussi : $\begin{cases} a \equiv \alpha \ (n) \\ b \equiv \beta \ (n) \end{cases}$

d'après la proposition 3.2 on a :

$$\begin{cases} a \equiv \alpha \ (n) \\ b \equiv \beta \ (n) \end{cases} \Rightarrow \begin{cases} a+b \equiv \alpha + \beta \ (n) \\ a.b \equiv \alpha\beta \ (n) \end{cases}$$

3.3 - Théorème : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

démonstration

on rappelle qu'un corps est un anneau dans lequel tout élément différent de 0 est inversible

\- supposons n premier

soit $\dot{m} \in \mathbb{Z}/n\mathbb{Z}$, $\dot{m} \neq \dot{0}$ et soit $m \in \dot{m}$

$\dot{m} \neq \dot{0}$ signifie que n ne divise pas m ; comme n est premier on en déduit que $(n, m) = 1$

Par suite on peut appliquer Bezout (définition 2.3) :

$$\exists\, u, v \in \mathbb{Z} \quad , \quad un + vm = 1$$

cette dernière égalité se traduit dans $\mathbb{Z}/n\mathbb{Z}$ par : $\dot{v}\dot{m} = \dot{1}$

on a ainsi trouvé un inverse de $\dot{m}$ dans $\mathbb{Z}/n\mathbb{Z}$ (c'est $\dot{v}$)

donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

\- Supposons que n n'est pas premier :

alors il existe p premier et $q \in \mathbb{N}^*$ tels que : $p.q = n$ (d'après le théorème 2.6)

$$0 < p < n \quad \text{et} \quad 0 < q < n \quad \Rightarrow \quad \dot{p} \neq 0 \quad \text{et} \quad \dot{q} \neq 0$$

or : $p.q = n \iff \dot{p}.\dot{q} = \dot{0}$ dans $\mathbb{Z}/n\mathbb{Z}$

on a donc trouvé un couple de diviseurs de zéro dans $\mathbb{Z}/n\mathbb{Z}$

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.

Remarque : un corps est un anneau intègre (sans diviseurs de zéro) mais un anneau sans diviseurs de zéro n'est pas nécessairement un corps (ex : $\mathbb{Z}$!)
En revanche on peut montrer qu'un anneau intègre <u>fini</u> est un corps.

- Caractéristique d'un corps

Soit K un corps commutatif.
Considérons l'application $\varphi : \mathbb{Z} \to K$ définie par $\varphi(n) = n.1$
Cette application est un homomorphisme d'anneaux.
Par suite $\varphi(\mathbb{Z})$ est un sous-anneau de K
Ker φ est un idéal de $\mathbb{Z}$: on a donc $\text{Ker}\,\varphi = n.\mathbb{Z}$
On dit que n est la <u>caractéristique</u> du corps K

3.4 - Proposition : La caractéristique d'un corps est un nombre premier ou zéro

démonstration

Soit n la caractéristique du corps K
si $n \neq 0$, $\varphi(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$
comme $\varphi(\mathbb{Z})$ est un sous-anneau du corps K, $\varphi(\mathbb{Z})$ est intègre alors d'après la démonstration du théorème 3.3 : n est premier.

• Remarque : si K est un corps fini, sa caractéristique est non nulle (en effet $\varphi(\mathbb{Z})$ ne peut être isomorphe à $\mathbb{Z}$ qui est infini)

3.5 - Théorème : Le cardinal d'un corps fini est une puissance de sa caractéristique.

démonstration

Soit $L = \varphi(\mathbb{Z})$. On a vu que L est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, où $p = \text{car}\, K$ est premier
comme L est un sous-corps de K, K est un L-espace vectoriel
soit $\{\beta_1, \dots, \beta_n\}$ une base
Alors $\forall \beta \in K \quad \exists (\lambda_1, \dots, \lambda_n) \in L^n$ tq $\beta = \lambda_1\beta_1 + \dots + \lambda_n\beta_n$
on peut ainsi définir une bijection de $L^n \simeq (\mathbb{Z}/p\mathbb{Z})^n$ dans K
on en déduit : $\# K = p^n$

- Sous groupes des groupes cycliques finis

Soit G un groupe commutatif et soit H un sous-groupe de G

On cherche quels sont les sous-groupes de G/H.

Soit K un sous-groupe de G/H ; si π est la surjection canonique de G sur G/H $\tilde{K} = \pi^{-1}(K)$ est un sous-groupe de G qui contient H

Réciproquement : on considère l'ensemble des sous-groupes de G qui contiennent H : si L appartient à cet ensemble alors $\pi(L) = L/H$ est un sous-groupe de G/H

Ainsi π induit une bijection :

$$\{K \ / \ K \subset G/H\} \underset{\pi^{-1}}{\overset{\pi}{\rightleftarrows}} \{L \ / \ H \subset L \subset G\}$$

• Application : $G = \mathbb{Z}$, $H = m\mathbb{Z}$

si a divise m, $a\mathbb{Z} \supset m\mathbb{Z} \subset \mathbb{Z}$ on en déduit : $a\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/\frac{m}{a}\mathbb{Z}$

3.6. Théorème : Pour chaque diviseur a de m il y a exactement un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$ qui est d'ordre $\frac{m}{a}$: c'est le groupe cyclique engendré par $\dot{a} \in \mathbb{Z}/m\mathbb{Z}$.

• Remarque : Soit L le sous-groupe cyclique de $\mathbb{Z}/m\mathbb{Z}$ engendré par $\dot{a}$: pour tout $x \in H$ on a $\frac{m}{a} x \equiv 0$

Plus généralement cherchons à résoudre l'équation $n x \equiv 0$ dans $\mathbb{Z}/m\mathbb{Z}$

Dans $\mathbb{Z}/m\mathbb{Z}$ cette équation s'écrit : $n\dot{x} = \dot{0} \ (m)$

en particulier $\exists\, k$ tel que $nx = km$

Soit d le pgcd de m et n on a vu qu'alors $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$

si on pose $m' = \frac{m}{d}$, $n' = \frac{n}{d}$ avec $(m', n') = 1$

l'égalité $nx = km$ devient $n'x = km'$ soit encore $x = \ell m'$

où $\ell = \frac{k}{n'} \in \mathbb{N}$

en définitive on peut écrire $x = \ell \frac{m}{d}$: x est un multiple de $\frac{m}{d}$

d'où $\{\dot{x} \ / \ n\dot{x} = 0 \ (m)\} = \left\{\dot{\frac{m}{d}}, \dot{\frac{2m}{d}}, \dots, \dot{\frac{(d-1)m}{d}}\right\}$

or ceci est un groupe cyclique d'ordre d engendré par $\frac{m}{d}$ d'où

3.7. Proposition : dans $\mathbb{Z}/m\mathbb{Z}$ l'ensemble des éléments $\dot{x}$ tels que $n\dot{x} = 0$ est le sous-groupe cyclique d'ordre $d = \mathrm{pgcd}(m,n)$ engendré par $\frac{m}{d}$

. Remarque : A chaque élément g d'un groupe additif G on peut associer l'homomorphisme $\varphi_g : \mathbb{Z} \to G$ défini par $\varphi_g(n) = n.g$

on a donc $\mathrm{Hom}(\mathbb{Z}, G) \simeq G$

on vérifie immédiatement qu'on définit ainsi une bijection de $Hom(\mathbb{Z},G)$ dans G

De même à chaque élément g de G tel que $n.g = 0$ on peut associer l'homomorphisme $\varphi_g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ défini par $\varphi_g(\dot{m}) = m\varphi_g(\dot{1}) = mg$ on définit ainsi une bijection :

$$\{g \in G^+ \ / \ ng = 0\} \xrightarrow{\sim} Hom(\mathbb{Z}/n\mathbb{Z}, G)$$

La proposition 3.7 montre l'existence de l'isomorphisme :

$$Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z} \qquad \text{où } d = pgcd(m,n)$$

4 - La fonction d'Euler

- Définition

On considère le groupe cyclique d'ordre m : $\mathbb{Z}/m\mathbb{Z}$ et on se demande combien il y a d'éléments dans $\mathbb{Z}/m\mathbb{Z}$ d'ordre m exactement.

On cherche donc $\{y \ / \ my = 0 \text{ et } ny \neq 0, \forall n, 0<n<m\}$ qui s'identifie à $\{\dot{y} \ / \ (y,m) = 1\}$

4.0 - Définition : pour $m > 0$ on pose :

$$\varphi(m) = \#\{\dot{y} \in \mathbb{Z}/m\mathbb{Z} \ / \ (y,m) = 1\} = \#\{y \ / \ 0<y<m, (y,m) = 1\}$$

φ est la fonction d'Euler ; c'est une application de $\mathbb{N}^*$ dans $\mathbb{N}$.

• Les éléments d'ordre m dans $\mathbb{Z}/m\mathbb{Z}$ engendrent $\mathbb{Z}/m\mathbb{Z}$. Autrement dit $\varphi(m)$ est le nombre de générateurs du groupe cyclique $\mathbb{Z}/m\mathbb{Z}$.

- Propriété fondamentale de φ

4.1 - Théorème : $\sum_{d/m} \varphi(d) = m$

démonstration

dans $\mathbb{Z}/m\mathbb{Z}$, $\forall d, d/m$ $\varphi(d) = \#\{x \in \mathbb{Z}/m\mathbb{Z} \text{ d'ordre } d \text{ exactement}\}$

si on pose $C_k = \{x \text{ d'ordre } k \text{ exactement}\}$ $1 \leq k \leq m$:

$$\varphi(d) = \# C_d$$

et on a : $\mathbb{Z}/m\mathbb{Z} = C_1 \cup \ldots \cup C_d \cup \ldots \cup C_m$

• comme application de cette formule nous allons établir le théorème suivant :

4.2 - Théorème : Soit G un groupe commutatif d'ordre m tel que $\{x \ / \ dx = 0\}$ a au plus d éléments. Alors G est cyclique.

démonstration

soit $(C_d)_{d/m}$ la partition de G suivant les ordres des éléments

$$\#\left(\bigcup_{d'/d} C_{d'}\right) = \#\{x \in G / dx = 0\} \leq d \text{ par hypothèse}$$

Si G possède un élément d'ordre d exactement, alors on va montrer que G en possède $\varphi(d)$

En effet soit $y \in G$ un élément d'ordre d exactement

L'ensemble des multiples de y $\{0, y, 2y \dots (d-1)y\}$ est un sous-groupe de G isomorphe à $\mathbb{Z}/d\mathbb{Z}$: tous ses éléments vérifient l'équation $dx = 0$; comme cette équation est supposée avoir au plus d solutions, il n'y en a pas d'autres ; en particulier parmi ceux-là il y en a $\varphi(d)$ d'ordre d exactement.

Soit $\gamma(d) = \# C_d$ le nombre d'éléments d'ordre d dans G

on vient de voir que $\gamma(d) = \varphi(d)$ ou 0

comme $\sum_{d/m} \gamma(d) = m = \sum_{d/m} \varphi(d)$

on en déduit que : $\gamma(d) = \varphi(d)$ pour tout d/m

en particulier : $\gamma(m) = \varphi(m) \neq 0$ $(\varphi(m) \geq 1)$

Tout élément d'ordre m engendre le groupe.

Donc on a montré que G est cyclique.

- application : $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier ; $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe (à (p-1) éléments) pour la multiplication - Montrons que ce groupe est cyclique

En effet soit $d/(p-1)$; on regarde le nombre de solutions de l'équation $x^d = 1$; c'est aussi le nombre de racines du polynôme $x^d - 1 = 0$; or on sait que ce polynôme admet au plus d racines sur un corps commutatif quelconque.

on en déduit que le groupe considéré est cyclique.

Plus généralement on a :

4.3. Théorème : *Le groupe multiplicatif K^* d'un corps fini K est cyclique.*

- Calcul de φ

- calcul de $\varphi(p^n)$, p premier

$n = 1$ $\varphi(p) = \{$ nombres premiers avec p et inférieurs à p $\}$

$$\varphi(p) = p - 1$$

$n \neq 1$ $\varphi(p^n) = \{$ nombres $< p^n$ et non multiples de $p\}$

$= \{$ nombres $< p^n\} - \{$ nombres $< p^n$ multiples de $p\}$

or les multiples de p inférieurs à p^n sont : $p, 2p, \dots (p^{n-1}-1)p$

il y en a $p^{n-1}-1$

d'autre part des nombres inférieurs à p^n il y en a $p^n - 1$

d'où $\varphi(p^n) = (p^n-1) - (p^{n-1}-1) = p^n - p^{n-1}$

$$\boxed{\varphi(p^n) = p^n\left(1-\frac{1}{p}\right)}$$

• **4.4 - Théorème :** si a et b sont premiers entre eux :

$$\boxed{\varphi(ab) = \varphi(a)\,.\,\varphi(b)}$$

La démonstration sera faite un peu plus loin

4.5 - Corollaire : si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ alors :

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right) = n \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

$$\boxed{\frac{\varphi(n)}{n} = \prod_{\substack{p/n \\ p \text{ premier}}} \left(1-\frac{1}{p}\right)}$$

Pour la démonstration du théorème nous allons avoir besoin d'un autre théorème :

4.6 - Théorème chinois : si $(a,b) = 1$ l'anneau $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

démonstration de ce théorème

Soit l'application $\phi : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

pour démontrer le théorème il faut montrer que :

$$(a,b) = 1 \iff \phi \text{ bijectif}$$

En fait il suffit de montrer que ϕ est injectif car les 2 anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ont le même nombre d'éléments.

Considérons $\operatorname{Ker}\phi = \left\{ x \in \mathbb{Z}/ab\mathbb{Z} \;/\; \begin{matrix} x \equiv 0 \ (a) \\ x \equiv 0 \ (b) \end{matrix} \right\}$

$= \left\{ x \in \mathbb{Z}/ab\mathbb{Z} \;/\; \begin{matrix} x = \lambda a \\ x = \mu b \end{matrix} \right\}$

or $\begin{cases} x = \lambda a \\ x = \mu b \end{cases} \iff x = k\,.\,\text{ppcm}(a,b)$

mais $\text{ppcm}(a,b) = \frac{ab}{d}$ où $d = \text{pgcd}(a,b)$

on en déduit : $\operatorname{Ker}\phi = \left\{ x \in \mathbb{Z}/ab\mathbb{Z} \;/\; x = k\frac{ab}{d} \right\}$

$= \left\{ \frac{ab}{d}, \frac{2ab}{d} \dots\dots (d-1)\frac{ab}{d} \right\}$

on voit alors que $\operatorname{Ker}\phi$ est un groupe cyclique d'ordre d

$$\operatorname{Ker}\phi \simeq \mathbb{Z}/d\mathbb{Z} \quad (\simeq \tfrac{ab}{d}\mathbb{Z}/ab\mathbb{Z})$$

et par suite : $d = 1 \Leftrightarrow \operatorname{Ker}\phi = \{0\}$

donc ϕ est injectif - le théorème est démontré

démonstration du théorème 4.4

D'après le théorème précédent (4.6) on sait que si $(a,b) = 1$

il existe un isomorphisme d'anneau $\mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

or $(\mathbb{Z}/ab\mathbb{Z})^*$ est un groupe d'ordre $\varphi(a.b)$

$(\mathbb{Z}/a\mathbb{Z})^*$ ———— $\varphi(a)$

$(\mathbb{Z}/b\mathbb{Z})^*$ ———— $\varphi(b)$

d'où $\varphi(a.b) = \varphi(a).\varphi(b)$

- Généralisation du théorème chinois

. Nous avons considéré dans ce qui précède :

$$\phi : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Dans le cas général $\operatorname{pgcd}(a,b) = d$

Nous avons donc : $\operatorname{Ker}\phi \simeq \mathbb{Z}/d\mathbb{Z}$

On peut alors donner une factorisation de ϕ selon le diagramme suivant :

$$\begin{array}{ccc} \mathbb{Z}/ab\mathbb{Z} & \xrightarrow{\phi} & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \pi \downarrow & & \uparrow \bar{\phi} \\ (\mathbb{Z}/ab\mathbb{Z})/\operatorname{Ker}\phi & \xrightarrow{\simeq} & \mathbb{Z}/\mu\mathbb{Z} \end{array}$$

où $\mu = \operatorname{ppcm}(a,b)$

π est la surjection canonique

$\bar{\phi}$ est une application injective et une bijection de $\mathbb{Z}/\mu\mathbb{Z}$ sur $\operatorname{Im}\phi$

. Considérons maintenant l'application :

$$\begin{aligned} \delta : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\longrightarrow \mathbb{Z}/d\mathbb{Z} \\ (x,y) &\longrightarrow (\dot{x} - \dot{y}) \end{aligned}$$

4.7 - Proposition : $\operatorname{Ker}\delta = \operatorname{Im}\phi$

démonstration

. $\operatorname{Im}\phi \subset \operatorname{Ker}\delta$ en effet :

$\forall \dot{x} \in \mathbb{Z}/ab\mathbb{Z}$ $\quad \delta\circ\phi(\dot{x}) = \delta(\phi(\dot{x}_{ab})) = \delta(\dot{x}_a, \dot{x}_b) = (\dot{x} - \dot{x})_d = 0$

. $\operatorname{Ker}\delta \subset \operatorname{Im}\phi$ car :

considérons $(\dot{y}_a, \dot{z}_b) \in \operatorname{Ker}\delta$; alors $(\dot{y} - \dot{z})_d = 0$ c'est à dire $d \mid y - z$

or $d = \operatorname{pgcd}(a,b) \Rightarrow \exists\, u, v \in \mathbb{Z}$ tq $d = ub + va$ et par suite $y - z = kd = k(ub + va)$

on peut donc trouver $x \in \mathbb{Z}$ tq $\phi(\dot{x}_{ab}) = (\dot{y}_a, \dot{z}_b)$; il suffit de poser $\begin{cases} x = y - kva \\ x = z + kub \end{cases}$

. On traduit ce résultat en disant que la suite ci-dessous est <u>exacte</u>

$$0 \to \mathbb{Z}/d\mathbb{Z} \xrightarrow{i} \mathbb{Z}/ab\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \xrightarrow{\delta} \mathbb{Z}/d\mathbb{Z} \to 0$$

$$\dot{\imath} \to \dot{\overline{\frac{mn}{d}}} \qquad (x, y) \to (\dot{x} - \dot{y})_{\text{mod } d}$$

En outre tout ce qui précède peut être rassemblé dans le diagramme suivant :

$$\mathbb{Z}/\mu\mathbb{Z}$$

$$0 \to \mathbb{Z}/d\mathbb{Z} \xrightarrow{i} \mathbb{Z}/ab\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \xrightarrow{\delta} \mathbb{Z}/d\mathbb{Z} \to 0$$

(avec $\pi : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/\mu\mathbb{Z}$ et $\overline{\Phi} : \mathbb{Z}/\mu\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$)

. Interprétation : résolution des systèmes de congruence

Considérons le problème suivant :

trouver $x \in \mathbb{Z}$ tel que $\begin{cases} x \equiv y & (a) \\ x \equiv z & (b) \end{cases}$

ce problème est équivalent au suivant :

trouver $x \in \mathbb{Z}$ tel que $\overline{\Phi}(\dot{x}_{(\mu)}) = (\dot{y}_{(a)}, \dot{z}_{(b)})$

Pour savoir s'il admet des solutions on regarde si $(\dot{y}_{(a)}, \dot{z}_{(b)}) \in \operatorname{Im} \overline{\Phi}$

or $\operatorname{Im} \overline{\Phi} = \operatorname{Im} \phi$ et d'après la proposition 4.7 $\operatorname{Im} \overline{\Phi} = \operatorname{Im} \phi = \operatorname{Ker} \delta$

on regarde donc si $(\dot{y}_{(a)}, \dot{z}_{(b)}) \in \operatorname{Ker} \delta$

Par suite on aura des solutions si d divise $y - z$

D'autre part si x et x' sont solutions : $\overline{\Phi}(\dot{x}_{(\mu)}) = \overline{\Phi}(\dot{x}'_{(\mu)})$

c'est à dire $x \equiv x' \ (\mu)$

D'où : on aura une solution unique modulo μ et d solutions modulo ab

Exemple : Résoudre le système $\begin{cases} 6x \equiv 8 & (28) \\ 5x \equiv 9 & (21) \end{cases}$ (S)

on se ramène à un système de la forme $\begin{cases} x \equiv y & (a) \\ x \equiv z & (b) \end{cases}$

$$(S) \Leftrightarrow \begin{cases} 3x \equiv 4 & (14) \\ 5x \equiv 9 & (21) \end{cases} \Leftrightarrow \begin{cases} x \equiv 6 & (14) \\ x \equiv 6 & (21) \end{cases}$$

Ce système admet des solutions

Il admet une solution unique modulo ppcm $(14, 21) = 42$ qui est 6

$$x \equiv 6 \ (42)$$

et il admet 7 solutions modulo $14 \times 21 = 294$

- Chapitre III -

Groupes abéliens de type fini

1 - Définitions et premières propriétés

- Systèmes générateurs, systèmes libres dans un groupe

Soit G un groupe abélien.

1.1 - Définition : Soit $(g_1, \dots g_n)$ une suite d'éléments de G ; on dit que la suite $(g_i)_{i=1 \dots n}$ est un système de générateurs de G si et seulement si l'application $f : \mathbb{Z}^n \to G$ définie par : [même définition si $(g_1, \dots, g_n, \dots)$ infini]
$f(a_1 \dots a_n) = \sum_{i=1}^{n} a_i g_i$ est surjective.

1.2 - Définition : La suite $(g_1 \dots g_n)$ d'éléments de G est un système libre de G si et seulement si l'application $f : \mathbb{Z}^n \to G$ définie par $f(a_1 \dots a_n) = \sum_{i=1}^{n} a_i g_i$ est injective.

1.3 - Définition : Si la suite $(g_1, \dots g_n)$ d'éléments de G constitue un système générateur et libre de G alors $(g_1, \dots g_n)$ est une base du groupe abélien G.

Cela revient à dire que l'application $f : \mathbb{Z}^n \to G$ est bijective.

- Groupes abéliens de type fini

1.4 - Définition : On dit qu'un groupe abélien G est de type fini si et seulement s'il possède un système fini de générateurs.

Exemples : . Tout groupe G fini est un groupe abélien de type fini.

. Il existe aussi des groupes abéliens de type fini qui ne sont pas finis ; $\mathbb{Z}, \mathbb{Z}^2, \dots, \mathbb{Z}^n$ $\forall n \in \mathbb{N}$.

Remarque : $\mathbb{Q}$ considéré comme groupe abélien ne possède pas de système de générateurs fini : ce n'est pas un groupe abélien de type fini.

1.5 - Proposition : Un groupe abélien G est de type fini s'il possède un sous-groupe H de type fini tel que le groupe quotient G/H soit encore de type fini.

démonstration

Par hypothèse H est de type fini donc il possède un système de générateurs : $(h_1, \dots, h_m)$, $h_i \in H \ \forall i = 1, \dots m$

G/H est aussi supposé de type fini donc il possède également un système de générateurs : $(\bar{g}_1 \dots \bar{g}_n)$, $\bar{g}_i \in G/H \ \forall i = 1, \dots n$

soit $(g_1, \dots g_n)$, $g_i \in G$ un système de représentants des $\bar{g}_i$

On veut montrer que G est de type fini ; considérons $x \in G$; $\bar{x} \in G/H$: nous pouvons écrire $\bar{x} = \sum_{i=1}^{n} a_i \bar{g}_i$, $a_i \in \mathbb{Z}$

D'autre part si on considère les représentants on a $x - \sum_{i=1}^{n} a_i g_i \in H$

d'où $x - \sum_{i=1}^{n} a_i g_i = \sum_{i=1}^{m} b_i h_i$, $b_i \in \mathbb{Z}$

on en déduit : $x = \sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{m} b_i h_i$

G est donc engendré par le système $(g_1 \dots g_n, h_1 \dots h_m)$ à $m+n$ éléments : G est de type fini.

Bonne démonstration

1.6 - Théorème : Tout sous-groupe H d'un groupe abélien de type fini G est encore de type fini.

démonstration

G étant de type fini, il possède un système fini de générateurs, soit $(g_1, \dots g_n)$ ce système.

Nous allons faire un raisonnement par récurrence sur n.

. pour $n = 1$: si G est engendré par un seul élément g, alors G est cyclique, par suite H sous-groupe de G est aussi cyclique il est donc également engendré par un élément (pas nécessairement le même) on en déduit que H est de type fini.

. supposons maintenant que c'est vrai pour $n-1$

. montrons que c'est encore vrai pour n ; soit G' le sous-groupe de G engendré par les $n-1$ éléments : $g_1, g_2 \dots g_{n-1}$

Considérons $H' = G' \cap H$; H' est un sous-groupe de G' donc d'après l'hypothèse de récurrence H' est de type fini, engendré par au plus $(n-1)$ éléments.

Considérons le groupe quotient H/H' ; l'inclusion $H \hookrightarrow G$ induit une injection du groupe H/H' dans le groupe quotient G/G' ; en effet on a :

$$\begin{array}{ccc} H/H' & \longrightarrow & G/G' \\ s_1 \uparrow & \overset{p}{\nearrow} & \uparrow s_2 \\ H & \underset{i}{\hookrightarrow} & G \end{array}$$

où p est un homomorphisme

et $\ker p = \{h \in H \,/\, h \in G'\} = H \cap G' = H'$
Or G/G' est cyclique car engendré par l'élément $\bar{g}_n$ ($= g_n + G'$)
on en déduit que H/H' est cyclique, donc de type fini
Il ne reste plus qu'à appliquer la proposition 1.5 pour conclure que H est de type fini (engendré par au plus n éléments)

- Groupes Libres de type fini

1.7 - Définition : on dit qu'un groupe abélien G est libre si et seulement s'il possède une base c'est à dire une partie formée d'éléments de G l'engendrant et libre.
Le cardinal de la base s'appelle le rang du groupe. (on démontre en effet que deux bases d'un même groupe libre ont même cardinal)

• Dans ce qui suit nous allons considérer les groupes abéliens libres de type fini.
Exemples : $\mathbb{Z}, \mathbb{Z}^2, \dots, \mathbb{Z}^n$ $\forall n \in \mathbb{N}$ sont des groupes abéliens libres de type fini

Remarque : Il existe des groupes libres non de type fini comme $\mathbb{Z}[X]$

1.8 - Proposition : Tout groupe abélien libre de rang n est isomorphe à $\mathbb{Z}^n$.

démonstration
D'après la définition 1.3, si $(g_1 \dots g_n)$ constitue une base de G alors l'application

$$f : \mathbb{Z}^n \to G, \quad (a_1 \dots a_n) \to \sum_{i=1}^{n} a_i g_i$$

est bijective
on en déduit un isomorphisme de groupe de $\mathbb{Z}^n$ dans G

conséquence : un groupe fini n'est jamais libre.

1.9 - Théorème : Tout sous-groupe de $\mathbb{Z}^n$ est libre et de rang inférieur ou égal à n.

démonstration
Il faut montrer : $\forall H \subset \mathbb{Z}^n$, $\exists\, m$, $m \le n$ tq $H \simeq \mathbb{Z}^m$
Nous allons faire une récurrence sur n

. pour $n = 1$: Soit H un sous-groupe de $\mathbb{Z}$; nous avons vu (ch II) que tout sous groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$, $a \in \mathbb{N}$
Nous pouvons donc définir un isomorphisme : $\mathbb{Z} \longrightarrow H$
$m \longrightarrow m.a$
Et par suite H est libre

. supposons $H \subset \mathbb{Z}^{n-1} \Rightarrow \exists\ m \leq n-1$ tq $H \simeq \mathbb{Z}^m$

. montrons que c'est encore vrai dans $\mathbb{Z}^n$

Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{Z}^n$: $e_1 = (1,0\cdots 0)$ .... $e_n = (0, \cdots 0, 1)$
Considérons G' le groupe engendré par $(e_1 \dots e_{n-1})$ qui est isomorphe à $\mathbb{Z}^{n-1}$.

$G' \cap H = H'$, H' est alors un sous-groupe de $\mathbb{Z}^{n-1}$ et on peut par conséquent lui appliquer l'hypothèse de récurrence : H' est libre de rang $\ell \leq n-1$. Soit $(y_1 \dots y_\ell)$ une base de H'.
Considérons maintenant H/H' ; il existe une injection de H/H' dans G/G' or $G/G' = \mathbb{Z}^n / \mathbb{Z}^{n-1} = \mathbb{Z}\,\bar{e}_n$ c'est à dire que G/G' est libre de rang 1 . Par suite H/H' est aussi libre de rang 1
Soit $\bar{y}_n$ un générateur de H/H' on a : $\exists\, a_n \in \mathbb{N}$ tq $\bar{y}_n = a_n \bar{e}_n$
Un représentant quelconque de $\bar{y}_n$ s'écrit $y_n = a_n e_n + h'$ $h' \in H'$
Montrons que $\{y_1 \dots y_\ell\} \cup \{y_n\}$ est une base de H.
On sait déjà que c'est un système de générateurs (d'après 1.5) .
Il faut montrer qu'il est libre c'est à dire :

$$z = \alpha_1 y_1 + \alpha_2 y_2 + \dots + \alpha_\ell y_\ell + \alpha_n y_n = 0 \Rightarrow \alpha_1 = 0, \dots \alpha_\ell = 0, \alpha_n = 0$$

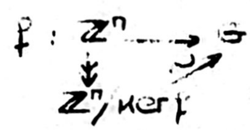
comme $\alpha_1 y_1 + \dots + \alpha_\ell y_\ell \in H'$ si on prend la classe de l'élément z modulo H' il vient : $\alpha_n \bar{y}_n = 0$ d'où $\alpha_n = 0$
D'autre part comme $(y_1 \dots y_\ell)$ est une base de H' , tous les α_i pour $i = 1 \dots \ell$ sont nuls.
Donc c'est bien un système libre .

1.10 - Proposition : Un groupe est de type fini si et seulement si c'est un quotient d'un groupe libre de type fini

démonstration

Soit G un groupe de type fini ; il possède un système fini de générateurs $(g_1 \dots g_n)$ donc par définition (1.1) il existe une surjection f de $\mathbb{Z}^n$ dans G .

on en déduit un isomorphisme de $\mathbb{Z}^n / \mathrm{Ker}\, f$ dans G



Réciproquement c'est évident.

. Le but de ce chapitre est d'étudier la structure des groupes abéliens de type fini.

Soit G un groupe abélien de type fini quelconque (non nécessairement libre) ; nous avons vu qu'il existait une surjection $f : \mathbb{Z}^n \to G$ et que $G \simeq \mathbb{Z}^n / \mathrm{Ker}\, \varphi$. Mais $\mathrm{Ker}\, \varphi$ est un sous groupe de $\mathbb{Z}^n$ et d'après (1.9) il va être libre de rang $m \leq n$ $(\mathrm{Ker}\, \varphi \simeq \mathbb{Z}^m)$

D'où pour étudier la structure d'un groupe abélien de type fini G, il suffira d'étudier les homomorphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$ $(m \leq n)$

En particulier ces homomorphismes sont caractérisés par une matrice A à n lignes et m colonnes d'où l'étude qui va suivre.

2. Matrices à coefficients dans $\mathbb{Z}$

- Généralités

. On considère l'ensemble des homomorphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$.

A tout homomorphisme $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}^n)$ correspond une matrice à n lignes et m colonnes à coefficients dans $\mathbb{Z}$.

. matrices équivalentes

2.1 - Définition : Soient M et M' 2 matrices $n \times m$ à coefficients dans $\mathbb{Z}$. On dit que M et M' sont équivalentes si et seulement s'il existe une matrice S $m \times m$ et une matrice T $n \times n$ toutes deux à coefficients dans $\mathbb{Z}$ et inversibles telles que : $M' = S.M.T$

Ceci peut aussi se traduire en disant que M et M' représentent le même homomorphisme exprimé dans 2 bases différentes.

2.2. Théorème : Pour toute matrice M, $n \times m$ à coefficients dans $\mathbb{Z}$ il existe 2 matrices S et T également à coefficients dans $\mathbb{Z}$ inversibles telles que la matrice produit S M T soit diagonale.

La démonstration de ce théorème sera faite dans les pages suivantes.

– Transformations élémentaires

2.3 - Définition : on appelle transformation élémentaire sur une matrice X à coefficients dans $\mathbb{Z}$ l'une des opérations suivantes :

- l'addition à une ligne (resp. colonne) d'un multiple d'une autre ligne (resp colonne)
- les permutation de lignes ou de colonnes
- les changement de signe d'une ligne ou d'une colonne.

Toute transformation élémentaire transforme X en une matrice équivalente.

• Etudions séparément chaque type de transformations élémentaires :

– l'addition à une ligne (resp colonne) d'un multiple d'une autre ligne (resp colonne)

considérons la matrice :

$$X = \begin{pmatrix} \cdots & a_{1i} & \cdots & a_{1j} & \cdots \\ \cdots & a_{2i} & \cdots & a_{2j} & \cdots \\ & \vdots & & \vdots & \\ \cdots & a_{ni} & \cdots & a_{nj} & \cdots \end{pmatrix} \qquad a_{ij} \in \mathbb{Z} \quad \forall i, \forall j$$

et considérons l'opération qui consiste à ajouter à la i^{eme} colonne λ fois la j^{ieme} colonne ; nous noterons cette opération $A^c(i+\lambda j)$.

La matrice X devient :

$$X' = A^c(i+\lambda j)(X) = \begin{pmatrix} \cdots & a_{1i}+\lambda a_{1j} & \cdots & a_{1j} & \cdots \\ \cdots & a_{2i}+\lambda a_{2j} & \cdots & a_{2j} & \cdots \\ & \vdots & & \vdots & \\ \cdots & a_{ni}+\lambda a_{nj} & \cdots & a_{nj} & \cdots \end{pmatrix}$$

De même on peut considérer l'opération qui consiste à ajouter à la i^{eme} ligne λ fois la j^{ieme} ligne ; l'opération est alors notée $A^L(i+\lambda j)$

et la matrice X devient :

$$X'' = A^L(i+\lambda j)(X) = \begin{pmatrix} \vdots & & \vdots \\ a_{i1}+\lambda a_{j1} & \cdots\cdots & a_{in}+\lambda a_{jn} \\ a_{j1} & \cdots\cdots & a_{jn} \\ \vdots & & \vdots \end{pmatrix}$$

Vérifions que les matrices obtenues par ces transformations élémentaires sont bien équivalentes à la matrice initiale X.

. dans le premier cas (opération sur les colonnes) on est passé de la matrice X à la matrice X′ en multipliant à droite X par la matrice :

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & & \lambda & \ddots \\ & & & & 1 \end{pmatrix} = I + \lambda . \delta_{ji} \qquad (\det = 1)$$

(élément λ en ligne j, colonne i)

. dans le second cas (opération sur les lignes) on est passé de la matrice X à la matrice X″ en multipliant à gauche X par cette même matrice $I+\lambda\delta_{ji}$

Or la matrice $I+\lambda\delta_{ji}$ est une matrice à coefficients dans $\mathbb{Z}$ inversible ;

(Son inverse est d'ailleurs la matrice $I - \lambda \delta_{ji}$)

on a :

$$X' = A^c(i+\lambda j)(X) = X \cdot (I + \lambda \delta_{ji})$$

$$X'' = A^L(i+\lambda j)(X) = (I + \lambda \delta_{ji}) \cdot X$$

on voit ainsi que les matrices X et X' d'une part, X et X'' d'autre part sont bien équivalentes.

- les permutations de lignes ou de colonnes

on considère toujours la matrice :

$$X = \begin{pmatrix} a_{i1} & \dots & a_{in} \\ a_{j1} & \dots & a_{jn} \end{pmatrix}$$

Soit $\delta^c(i,j)$ l'opération qui consiste à permuter les colonnes i et j et soit $\delta^L(i,j)$ l'opération qui consiste à permuter les lignes i et j.

De même que précédemment vérifions que ces opérations transforment X en une matrice équivalente.

. dans le premier cas (permutation des colonnes) on passe de la matrice X à la matrice $X' = \delta^c(i,j)(X)$ en multipliant à droite X par la matrice de la permutation :

$$J = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & \cdots & 1 \\ & & & \vdots & 1 & \vdots \\ & & & 1 & \cdots & 0 \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}$$

c'est la matrice identité dans laquelle on a permuté les colonnes i et j

. dans le second cas (permutation des lignes) on passe de la matrice X à la matrice $X'' = \delta^L(i,j)(X)$ en multipliant à gauche X par cette même matrice J.

La matrice J est une matrice à coefficients dans $\mathbb{Z}$, inversible. ($J^{-1} = J$)

on a :

$$X' = \delta^c(i,j)(X) = X \cdot J$$

$$X'' = \delta^L(i,j)(X) = J \cdot X$$

Donc les matrices X et X' d'une part, X et X'' d'autre part sont bien équivalentes.

- les changements de signe d'une ligne ou d'une colonne

on considère encore la matrice X.

on appelle $\sigma^c(i)$ l'opération qui consiste à changer de signe les termes de la colonne i, et $\sigma^L(i)$ celle qui consiste à changer de signe les termes de la ligne i.

on vérifie que les matrices obtenues par ces transformations sont équivalentes à X :

. dans le premier cas on passe de la matrice X à la matrice $X' = \sigma^c(i)(X)$ en multipliant à droite X par la matrice :

$$S = \begin{pmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & -1 & & \\ & & & & 1 & \\ 0 & & & & & \ddots \; 1 \end{pmatrix}$$

(le coefficient -1 étant à la colonne i)

. dans le second cas on passe de la matrice X à la matrice $X'' = \sigma^L(i)(X)$ en multipliant à gauche X par cette même matrice S.

La matrice S est une matrice à coefficients dans $\mathbb{Z}$ inversible ($S^{-1} = S$)

on a : $X' = \sigma^c(i)(X) = X.S$

$X'' = \sigma^L(i)(X) = S.X$

Les matrices X et X', X et X'' sont bien équivalentes

– Diagonalisation d'une matrice à coefficients dans $\mathbb{Z}$

2.4 - Théorème : Soit f un homomorphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$. Considérons $(e_1 \dots e_m)$ la base canonique dans $\mathbb{Z}^m$; soit alors $A = (f(e_1), \dots, f(e_i), \dots)$ la matrice de f, matrice $n \times m$ à coefficients dans $\mathbb{Z}$. Il existe une suite d'opérations élémentaires qui transforme la matrice A en une matrice de la forme :

$$\begin{pmatrix} d & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B = (b_{ij}) & \\ 0 & & & \end{pmatrix}$$ où d divise les b_{ij} $\forall i, \forall j$

Et de plus d est le p.g.c.d des a_{ij} coefficients de A

. Avant la démonstration une remarque préliminaire :

2.5 - Remarque : Une transformation élémentaire ne change pas le p.g.c.d des coefficients d'une matrice (à coefficients dans $\mathbb{Z}$)

démonstration

Soit A une matrice à coefficients dans $\mathbb{Z}$ et A' sa transformée par une opération élémentaire.

Il faut montrer que $\text{pgcd}(a_{ij}) = \text{pgcd}(a'_{ij})$ où $A = (a_{ij})$, $A' = (a'_{ij})$

considérons par exemple comme transformation élémentaire une combinaison linéaire de colonnes :

on a alors : $$\begin{pmatrix} a'_{ij} \end{pmatrix} = \begin{pmatrix} a_{1k} \dots a_{ik} + \alpha a_{jk} \dots a_{jk} \dots a_{mk} \end{pmatrix}_{k = 1, \dots n}$$

si un nombre divise a_{jk} et $a_{ik} + \alpha a_{jk}$ il divise forcément a_{ik}

on déduit : $\text{pgcd}_{\substack{i=1\dots m\\ j=1\dots n}}(a'_{ij}) = \text{pgcd}_{k=1\dots n}(a_{1k} \dots a_{ik}+\lambda a_{jk} \dots a_{jk} \dots a_{mk}) = \text{pgcd}_{\substack{i=1\dots m\\ j=1\dots n}}(a_{ij})$

la démonstration est encore plus évidente pour les autres transformations élémentaires.

démonstration du théorème 2.4

Considérons l'ensemble E des coefficients de toutes les matrices que l'on peut déduire de A par une suite de transformations élémentaires. Si A n'est pas la matrice nulle E admet un plus petit élément positif non nul a ; comme $x \in E$ entraine $-x \in E$ on a : $x \in E$ et $|x| < a \Rightarrow x = 0$

Démontrons que $a = d$ où d est le pgcd des a_{ij}

1) montrons que d divise a

D'après la remarque on sait que le pgcd se conserve dans toute transformation élémentaire. En particulier si A' est la matrice dans laquelle a figure d est encore le pgcd de A' puisque cette matrice est déduite de A par une suite de transformations élémentaires. Donc d divise a

2) montrons que a divise tous les a_{ij}

Il suffit de montrer que a divise tous les coefficients d'une matrice quelconque déduite de A par transformations élémentaires. Considérons donc la matrice A' dans laquelle a figure. a étant le plus petit coefficient de A', on peut faire la division euclidienne de tous les autres éléments de A' par a.

Supposons que a se trouve à la place (i,j) dans A', pour tout élément a'_{ik} de la même ligne que a, en particulier,

$$\exists q, \exists r \text{ tels que } a'_{ik} = a.q + r \qquad 0 \leq r < a$$

si on soustrait maintenant de la $k^{\text{ième}}$ colonne q fois la $j^{\text{ième}}$ colonne à la place (i,k) il va rester r ; or $r < a$ ce qui implique $r = 0$

Ainsi par division euclidienne on peut faire apparaitre des "0" partout sur la ligne à laquelle a appartient.

De la même manière on peut faire apparaitre des "0" partout sur la colonne à laquelle a appartient.

On se ramène alors à une matrice A'' équivalente à A' :

$$A'' = \begin{pmatrix} & & 0 & & \\ & & \vdots & & \\ 0 & \cdots 0 & a & 0 \cdots & 0 \\ & & \vdots & & \\ & & 0 & & \end{pmatrix}$$

Et enfin à la matrice A''' :

$$A''' = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

(obtenue par permutation de lignes et de colonnes sur A'')

Il reste maintenant à montrer que a divise un coefficient b quelconque de B.

Pour cela nous allons transformer la matrice A''' en ajoutant la 1ère colonne à la colonne qui contient b, on obtient :

$$\begin{pmatrix} a & 0 \cdots & a & \cdots 0 \\ 0 & & & \\ \vdots & & b & \\ 0 & & & \end{pmatrix}$$

Pour les mêmes raisons que précédemment on peut écrire :

$$b = qa + r \quad \text{avec} \quad 0 \leq r < a$$

et comme $r < a$ on a encore $r = 0$

Donc a divise b quelconque dans B ; d'où le théorème.

2.6 - Théorème : Soit A une matrice $n \times m$ à coefficients dans $\mathbb{Z}$. Il existe une suite d'opérations élémentaires qui transforme A en une matrice de la forme :

$$\begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_k \end{pmatrix} \quad \text{où} \quad k = \inf(m,n)$$

avec d_1 divise d_2 ... etc, divise d_k

démonstration

Il suffit d'itérer le théorème 2.4.

2.7 - Propriété : Le produit $d_1 d_2$ divise le produit $d_i d_j$ pour tout $i \neq j$

• **Exemple** : considérons l'homomorphisme f, $\mathbb{Z}^2 \longrightarrow \mathbb{Z}$ défini par : $f(x,y) = ax + by$. A cet homomorphisme est associée la matrice $A = (a,b)$; le théorème 2.6 dit que cette matrice A peut être transformée par opérations élémentaires en une matrice $(d,0)$ où $d = \text{pgcd}(a,b)$

Remarquons ce que l'on fait, en fait, c'est l'algorithme d'Euclide pour trouver le pgcd de a et b.

De plus dire que (a,b) est équivalente à $(d,0)$ c'est la multiplier par une matrice 2×2 inversible :

$$(a \quad b)\begin{pmatrix} \alpha & u \\ \beta & v \end{pmatrix} = (d,0) \qquad \text{avec} \qquad \alpha v - \beta u = \pm 1$$

ce qui nous donne :

$$\begin{cases} \alpha a + \beta b = d & \text{(identité de Bezout)} \\ au + bv = 0 & \text{(noyau de l'application linéaire)} \end{cases}$$

On peut déterminer : u et v $\qquad u = -\frac{b}{d} \qquad v = \frac{a}{d}$

Et par suite déterminer la matrice $\begin{pmatrix} \alpha & u \\ \beta & v \end{pmatrix}$

Or trouver cette matrice c'est résoudre l'équation $ax + by = c$

• Remarque : Nous venons de montrer que toute matrice (rectangulaire) à coefficients dans $\mathbb{Z}$ est <u>équivalente</u> à une matrice diagonale. On se gardera de confondre cette diagonalisation avec celle des matrices d'endomorphisme (carrées) qui consiste à chercher une matrice carrée diagonale <u>semblable</u> à la matrice donnée.

La différence des 2 méthodes peut être mise en évidence par la comparaison des 2 diagrammes suivants :

①
$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^n \\ S\downarrow & & \downarrow T \\ \mathbb{Z}^m & \xrightarrow[A']{} & \mathbb{Z}^n \end{array}$$

A' est équivalente à A

$A' = TAS^{-1}$

②
$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^m \\ S\downarrow & & \downarrow S \\ \mathbb{Z}^m & \xrightarrow[A']{} & \mathbb{Z}^m \end{array}$$

A' est semblable à A

$A' = SAS^{-1}$

• Conséquences

2.8 . Théorème : Deux matrices qui peuvent être réduite à la même forme diagonale sont équivalentes.

Dans la suite nous verrons que ce théorème admet une réciproque

démonstration

Soient A et B 2 matrices $n \times m$ à coefficients dans $\mathbb{Z}$

D'après le théorème 2.5 A est équivalente à une matrice diagonale D_1, de même B est équivalente à une matrice diagonale D_2. Or par hypothèse $D_1 = D_2$. On en déduit que A et B sont équivalentes entre elles (elles sont équivalentes chacune de leur côté à une même matrice)

3. Caractérisation des diviseurs élémentaires
Théorème de structure des groupes abéliens de type fini

- Les diviseurs élémentaires

Soit $f \in Hom_{\mathbb{Z}}(\mathbb{Z}^m, \mathbb{Z}^n)$; Soit $A = (a_{ij})$ la matrice associée.
Dans le paragraphe précédent nous avons vu que toute matrice à coefficients dans $\mathbb{Z}$ est équivalente à une matrice diagonale ; donc A est équivalente à la matrice $\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{pmatrix}$ avec $k = \inf(m,n)$ et avec $d_1/d_2/\dots/d_k$

3.1 - Définition : Les $d_1 \dots d_k$ obtenus dans la matrice diagonale équivalente à A s'appellent les diviseurs élémentaires de A

• Propriétés :

- $d_1 = \text{pgcd}(a_{ij})$
- $d_1.d_2$ = pgcd des mineurs d'ordre 2 dans A
- $d_1.d_2.d_3$ = pgcd des mineurs d'ordre 3 dans A
- . . . .
- $d_1 \dots d_k$ = déterminant de A

Th. admis

• Remarque : Cette définition des diviseurs élémentaires suggère qu'ils dépendent de la matrice A . Nous allons voir qu'en fait ils ne dépendent que de l'homomorphisme f.

3.2 - Théorème : Les diviseurs élémentaires sont des invariants d'équivalence (autrement dit ils ne dépendent que de l'homomorphisme f)

démonstration

. Commençons par considérer $Hom(\mathbb{Z}^n, \mathbb{Z})$ l'ensemble des formes linéaires sur $\mathbb{Z}^n$. $Hom(\mathbb{Z}^n, \mathbb{Z})$ a une structure de groupe abélien de plus c'est un groupe abélien libre , par conséquent $Hom(\mathbb{Z}^n, \mathbb{Z}) \simeq \mathbb{Z}^n$
Soit $(\varepsilon_1 \dots \varepsilon_n)$ la base canonique de $\mathbb{Z}^n$ $(\varepsilon_1 = (1,0\dots0) \dots \varepsilon_n = (0\dots0\,1))$
Alors $\forall (a_1 \dots a_n) \in \mathbb{Z}^n$ on a $(a_1 \dots a_n) = \sum_1^n a_i \varepsilon_i$
Soit $(\varepsilon_1^* \dots \varepsilon_n^*)$ la base duale : $\varepsilon_1^*, \dots, \varepsilon_n^* \in Hom(\mathbb{Z}^n, \mathbb{Z})$
on pose par définition $\varepsilon_i^*(\varepsilon_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$
on a : $\varepsilon_i^*(a_1 \dots a_n) = a_i$
Toute forme linéaire est d'une manière unique une combinaison linéaire des ε_i^* on peut écrire :

$$Hom(\mathbb{Z}^n, \mathbb{Z}) = \mathbb{Z}\varepsilon_1^* \oplus \dots \oplus \mathbb{Z}\varepsilon_n^* .$$

Soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}$ une forme linéaire ;

$Im(f \circ \varphi)$ est un sous-groupe de $\mathbb{Z}$

L'ensemble $\sum_{\varphi \in Hom(\mathbb{Z}^n, \mathbb{Z})} \varphi \circ f(\mathbb{Z}^m)$ est aussi un sous-groupe de $\mathbb{Z}$ qui ne dépend que de f ; il est de la forme $k\mathbb{Z}$.

Montrons que $k = pgcd(a_{ij})$ (les a_{ij} étant les coef. de la matrice de f)

$$\sum_{\varphi} \varphi \circ f(\mathbb{Z}^m) = \sum_{i=1}^{n} e_i^* \circ f(\mathbb{Z}^m)$$

si on note $e_1 \dots e_m$ la base canonique de $\mathbb{Z}^m$ il vient :

$$\sum_{\varphi} \varphi \circ f(\mathbb{Z}^m) = \sum_{i=1}^{n}\sum_{j=1}^{m} \varepsilon_i^* \circ f(e_j)\,\mathbb{Z}$$

or $\varepsilon_i^*(f(e_j)) = a_{ij}$

donc

$$\sum_{\varphi} \varphi \circ f(\mathbb{Z}^m) = \sum_{ij} a_{ij}\mathbb{Z}$$

$$= d_1\mathbb{Z} \qquad \text{où} \quad d_1 = pgcd(a_{ij})$$

. Ensuite on considère $Hom(\mathbb{Z}^n \times \mathbb{Z}^n, \mathbb{Z}) \dots Hom(\mathbb{Z}^n \times \dots \times \mathbb{Z}^n, \mathbb{Z})$

Rappelons qu'une forme p-linéaire alternée sur $\mathbb{Z}^n$ est une application

$$g : \underbrace{\mathbb{Z}^n \times \mathbb{Z}^n \times \dots \times \mathbb{Z}^n}_{p} \longrightarrow \mathbb{Z}$$

qui a la propriété suivante :

$$g(x_1 \dots x_p) = (-1)^{\text{sign}\,\sigma} g(x_{\sigma(1)}, x_{\sigma(2)}, \dots x_{\sigma(p)})$$

la démonstration est la même : on regarde comment est engendrée une forme p-linéaire alternée g

on a :

$$\sum_{g \text{ p-lin.alt.}} g\big(f(\mathbb{Z}^m), \dots f(\mathbb{Z}^m)\big) = d_1 . d_2 \dots d_p \mathbb{Z}$$

. conséquences

3.3 - Théorème : Deux matrices A et A', $n \times m$ à coefficients dans $\mathbb{Z}$ sont équivalentes si et seulement si elles ont mêmes diviseurs élémentaires

démonstration

Deux matrices équivalentes représentent le même homomorphisme f.

Et comme nous venons de voir que les diviseurs élémentaires ne dépendent que de l'homomorphisme ils sont les mêmes pour les 2 matrices équivalentes

La réciproque a déjà été vue : c'est le théorème 2.8.

3.4 - Proposition : Deux matrices sont équivalentes si et seulement si il existe une suite de transformations élémentaires qui permet de passer de l'une à l'autre

démonstration

Dans un sens c'est évident puisqu'on sait que toute transformation élémentaire transforme une matrice A en une matrice équivalente A'. La réciproque vient du fait que les diviseurs élémentaires ne dépendent que de la classe d'équivalence ;

3.5 - Proposition : Deux matrices diagonales ne sont équivalentes que si elles sont égales.

démonstration

soit $D = \begin{pmatrix} d_1 & & & 0 \\ & d_2 & & \\ & & \ddots & \\ 0 & & & d_k \end{pmatrix}$ avec $d_1 \mid d_2 \mid \dots \mid d_k$

et soit $D' = \begin{pmatrix} d'_1 & & & 0 \\ & d'_2 & & \\ & & \ddots & \\ 0 & & & d'_k \end{pmatrix}$ avec $d'_1 \mid d'_2 \mid \dots \mid d'_k$

Alors $D \sim D' \Rightarrow d_i = d'_i \quad \forall i = 1 \dots k$

(puisque 2 matrices équivalentes ont mêmes diviseurs élémentaires)

- Structure des groupes abéliens de type fini.

3.6 - Théorème : Soit G un groupe abélien libre ($G \simeq \mathbb{Z}^m$) et soit H un sous-groupe de G. Il existe une base $(e_1, e_2, \dots e_m)$ de G et des entiers positifs $d_1, d_2, \dots d_m$ avec $d_1 \mid d_2 \mid \dots \mid d_m$ tels que $(d_1 e_1, \dots, d_k e_k)$ avec $k = \sup \{ j \mid d_j \neq 0 \}$ forme une base de H.

démonstration

Nous avons déjà vu que tout sous-groupe d'un groupe libre est libre (théorème 1.9). Par conséquent H est libre : il est isomorphe à $\mathbb{Z}^k$, $k \leq m$ (on suppose $G \simeq \mathbb{Z}^m$).

on a une injection $i : \underset{\mathbb{Z}^k}{\overset{H}{\wr\!\shortmid}} \hookrightarrow \underset{\mathbb{Z}^m}{\overset{G}{\wr\!\shortmid}}$ de matrice H.

Le théorème consiste à montrer qu'il existe une base dans G et une base dans H telles que la matrice puisse se réduire à une forme diagonale $\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{pmatrix}$;

or on sait, par ailleurs, que cette matrice existe : donc les bases existent.

Remarquons que, l'application i étant injective, les d_j, $j = 1 \dots k$, sont non nuls -

3.7 - Corollaire : Soit G un groupe abélien de type fini. G est isomorphe à une somme directe de groupes cycliques finis et d'un groupe libre de type fini

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r$$

avec $1 \neq d_1 | d_2 | \dots / d_k$.

r est alors le rang de G.

démonstration

G est un groupe abélien de type fini ; on sait qu'il existe un groupe libre de type fini L et un sous-groupe H de L tel que $G \simeq L/H$ (proposition 1.10)

Si on appelle π l'homomorphisme de L sur G, $H = \pi^{-1}(O_G)$ et on a :

$$H \hookrightarrow L \xrightarrow{\pi} G$$

or L est un groupe libre : $L \simeq \mathbb{Z}^m \simeq \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{m \text{ fois}}$

H est un sous-groupe d'un groupe libre ; il est donc libre

$H \simeq \mathbb{Z}^k \simeq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{k \text{ fois}}$

De plus, on peut lui appliquer le théorème 3.6. ; Pour tout élément $(x_1, \dots, x_k)$ dans H il existe un élément de la forme $(d_1x_1, \dots, d_kx_k, \underset{k+1}{0} \dots \underset{m}{0})$ dans L avec $d_1 / d_2 \dots / d_k$

Par suite on obtient :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^r \quad \text{où } r = m-k$$

avec $d_1 | d_2 \dots | d_k$

4 - Décomposition p-primaire d'un groupe abélien fini

- p-groupes

4.1 - Définition : on dit qu'un groupe G est un p-groupe si son cardinal est une puissance de p, p étant un nombre premier :

$$\# G = p^\alpha$$

Si G est abélien on dit plutôt qu'il est p-primaire.

• Problème : Comment détermine-t-on le nombre de groupes abéliens finis d'un ordre donné ?

Soit $\alpha(p^n)$ le nombre de groupes abéliens d'ordre p^n. (p premier)

Pour déterminer $\alpha(p^n)$ on utilise le corollaire 3.7 ; Par exemple :

. si $p = 2$, $n = 2$ on a $\alpha(4) = 2$ car on peut écrire :

$4 = 4$ et $4 = 2 \times 2$

Les 2 groupes d'ordre 4 sont $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

- si $p = 2$, $n = 3$ on a $\alpha(8) = 3$ car on peut écrire :

$8 = 8$, $8 = 2 \times 4$, $8 = 2 \times 2 \times 2$ -

Les 3 groupes d'ordre 8 sont $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

D'une façon générale :

- si p quelconque, n quelconque, il faut trouver toutes les suites $p^{n_1}, p^{n_2} \ldots\ldots p^{n_k}$ avec $n_1 \leqslant n_2 \leqslant \ldots \leqslant n_k$ et $\sum_{i=1}^{n_k} n_i = n$: ce nombre est le nombre de partitions possibles de n, noté $\mathcal{S}(n)$.

D'où : $\forall p$, p premier
$$\boxed{\alpha(p^n) = \mathcal{S}(n)}$$

On a une formule encore plus générale qui donne le nombre de groupes abéliens finis d'ordre n, n étant quelconque ; cette formule que nous ne démontrerons pas est la suivante :

$$\alpha(n) = \prod_{p \text{ premiers}} \mathcal{S}(\nu_p(n))$$

où $\nu_p(n) = \sup\{i \mid p^i \text{ divise } n\}$ est la valuation p-adique de n

on peut aussi l'écrire :

$$\alpha(n) = \prod_{p \text{ premiers}} p^{\nu_p(n)}$$

- Décomposition d'un groupe abélien fini

4.2. Théorème : Tout groupe abélien fini G est somme directe de groupes p-primaires où p parcourt l'ensemble des diviseurs premiers de l'ordre de G

$$G = \bigoplus_{p \in D} G_p$$

(Dans cette décomposition les groupes p-primaires G_p s'appellent les composantes p-primaires de G).

démonstration

Soit G un groupe fini d'ordre n

Appliquons lui le corollaire 3.7, on a :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots\ldots \oplus \mathbb{Z}/d_k\mathbb{Z} \quad \text{avec } d_1/d_2/\ldots/d_k$$

et $d_1.d_2 \ldots d_k = n$

Supposons que : $d_j = p_{j1}^{\alpha_{j1}} \cdot p_{j2}^{\alpha_{j2}} \ldots\ldots$ pour tout $j = 1 \ldots k$
avec p_{j1} premier

Alors d'après le théorème chinois :

$$\mathbb{Z}/d_j\mathbb{Z} = \mathbb{Z}/p_{j1}^{\alpha_{j1}}\mathbb{Z} \oplus \mathbb{Z}/p_{j2}^{\alpha_{j2}}\mathbb{Z} \oplus \ldots\ldots \quad \forall j = 1 \ldots k$$

on peut ainsi écrire :

$$G \simeq (\mathbb{Z}/p_{11}^{\alpha_{11}}\mathbb{Z} \oplus \mathbb{Z}/p_{12}^{\alpha_{12}}\mathbb{Z} \oplus \dots) \oplus \dots \oplus (\mathbb{Z}/p_{k1}^{\alpha_{k1}}\mathbb{Z} \oplus \mathbb{Z}/p_{k2}^{\alpha_{k2}} \oplus \dots)$$

Remarquons que comme $d_1 / d_2 / \dots / d_k$ on a les inclusions :

$$\{p_{1i},\ i=1,2\dots\} \subset \{p_{2i},\ i=1,2\dots\} \subset \dots \subset \{p_{ki},\ i=1,2\dots\}$$

D'où un regroupement possible des termes correspondants à un même nombre premier.

$$G \simeq (\mathbb{Z}/p_1^{\alpha_1} \oplus \mathbb{Z}/p_1^{\alpha_2} \oplus \dots) \oplus (\mathbb{Z}/p_2^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \oplus \dots) \oplus \dots$$

quel que soit j $(\mathbb{Z}/p_j^{\alpha_1}\mathbb{Z} \oplus \dots)$ est un groupe d'ordre p_j^{β}

c'est donc un p-groupe que nous noterons G_{p_j}

on obtient ainsi la décomposition de G :

$$G = G_{p_1} \oplus G_{p_2} \oplus \dots$$ où $p_1, p_2 \dots$ sont les diviseurs premiers de n

4.3 - Remarque : Dans la décomposition précédente, chaque composante p-primaire est elle-même une somme directe de p-groupes cycliques.

. Considérons le cas particulier où G est un groupe abélien d'ordre $n = a.b$ avec $(a,b) = 1$

$$G = G_a \oplus G_b$$

on peut écrire : $n = \underbrace{(p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell})}_{a} \underbrace{(p_{\ell+1}^{\alpha_{\ell+1}} \dots p_{k-\ell}^{\alpha_{k-\ell}})}_{b}$

d'où $G = (G_{p_1} \oplus \dots \oplus G_{p_\ell}) \oplus (G_{p_{\ell+1}} \oplus \dots \oplus G_{p_k})$

Tout ceci vient en réalité du fait que n'importe quel groupe peut s'écrire comme produit de groupes cycliques.

- Applications

. Nous savons que le groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}$ (p premier) que l'on note $(\mathbb{Z}/p\mathbb{Z})^*$ (ie ensemble des éléments inversibles) est un groupe cyclique d'ordre $p-1$

Nous sommes maintenant en mesure de démontrer :

4.4 - Théorème : Si p premier et $p \neq 2$ le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique pour tout $k \geq 1$

démonstration

$(\mathbb{Z}/p^k\mathbb{Z})^*$ est un groupe abélien fini d'ordre n avec :

$$n = \#(\mathbb{Z}/p^k\mathbb{Z})^* = \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

on se trouve dans la situation où $n = a.b$ avec $(a,b) = 1$
en effet ici $(p^{k-1}, p-1) = 1$
on peut donc écrire : $(\mathbb{Z}/p^k\mathbb{Z})^* = G_{p^{k-1}} \oplus G_{p-1}$
Pour montrer que $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique il nous suffira donc de montrer que $G_{p^{k-1}}$ et G_{p-1} sont cycliques. (compte tenu du théorème Chinois puisque $(p^{k-1}, p-1) = 1$)

- montrons que G_{p-1} est cyclique ; Pour cela il nous suffit de trouver un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$ et même un élément d'ordre un multiple de $p-1$
Nous savons qu'il existe un homomorphisme d'anneau surjectif

$$\varphi : \mathbb{Z}/p^k\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$$
$$\dot{x}\,(p^k) \longrightarrow \ddot{x}\,(p)$$

cette surjection induit un homomorphisme de groupe également surjectif

$$\bar{\varphi} : (\mathbb{Z}/p^k\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$

Autrement dit si on trouve un élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ cet élément aura pour ordre dans $(\mathbb{Z}/p^k\mathbb{Z})^*$ un multiple de $p-1$
or $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique donc il possède un élément d'ordre $p-1$
Cet élément engendre le facteur G_{p-1} qui est par conséquent cyclique.

- montrons maintenant que $G_{p^{k-1}}$ est cyclique ; pour cela montrons qu'il existe un élément d'ordre p^{k-1} dans $(\mathbb{Z}/p^k\mathbb{Z})^*$
Nous allons utiliser la remarque suivante :

$$\forall k \in \mathbb{N}, p \neq 2 \qquad (1+p)^{p^k} \equiv 1 + p^{k+1} \; (p^{k+2})$$

cette remarque se démontre par recurrence sur k
Elle donne : $(1+p)^{p^{k-1}} \equiv 1 + p^k \; (p^{k+1}) \qquad \equiv 1 \; (p^k)$
et $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \; (p^k) \qquad \not\equiv 1 \; (p^k)$
ceci montre que l'ordre de $1+p$ divise p^{k-1} et ne divise pas p^{k-2} donc donc son ordre est p^{k-1}
Cet élément engendre $G_{p^{k-1}}$ qui est donc cyclique.

4.5 - Théorème : si n est impair, le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique si et seulement si $n = p^\alpha$ avec p premier.

démonstration

Nous avons vu que le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ était cyclique pour p premier, $p \neq 2$ et pour tout $\ell \geq 1$ (c'est le théorème 4.4)

Réciproquement montrons que si le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique (n impair) alors $n = p^\alpha$

Pour cela démontrons la contraposée ; supposons $n = p^\alpha q^\beta \ldots$ (comme n est impair tous les nombres premiers qui figurent dans cette décomposition sont impairs)

on peut écrire :

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p^\alpha\mathbb{Z})^* \oplus (\mathbb{Z}/q^\beta\mathbb{Z})^* \oplus \ldots$$

or $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique et $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq p^{\alpha-1}(p-1)\mathbb{Z}$

de même pour les autres termes.

Ainsi $(\mathbb{Z}/n\mathbb{Z})^*$ est décomposable en produit de groupes cycliques mais comme p, q ... sont impairs, $(p-1), (q-1)$ ... sont pairs.

donc les $p^{\alpha-1}(p-1)$, $q^{\beta-1}(q-1)$ ... ne sont pas premiers entre eux puisqu'ils ont un facteur 2 en commun

Par suite $(\mathbb{Z}/n\mathbb{Z})^*$ n'est pas cyclique.

• cas particulier de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ lorsque $p = 2$

$(\mathbb{Z}/4\mathbb{Z})^*$ est cyclique d'ordre 2

$(\mathbb{Z}/8\mathbb{Z})^*$ n'est déjà plus cyclique. (car tous ses éléments sont d'ordre 2)

Donc on n'a aucune chance de trouver un élément d'ordre $2^{\ell-1}$ dans le groupe multiplicatif $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ pour $\ell > 2$ puisque c'est déjà faux pour $\ell = 3$

Par contre nous allons montrer qu'il y a toujours un élément d'ordre $2^{\ell-2}$ dans $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ pour $\ell \geq 3$

4.6- Proposition : Dans le groupe multiplicatif $(\mathbb{Z}/2^\ell\mathbb{Z})^*$, $\ell \geq 2$, tous les éléments sont d'ordre $2^{\ell-2}$.

démonstration

commençons par montrer que $\dot{5}$ est d'ordre $2^{\ell-2}$ dans $\mathbb{Z}/2^\ell\mathbb{Z}$

$$5^{2^k} = (1+4)^{2^k} \equiv 1 + 2^{k+2} \quad (2^{k+3})$$

$$(1+4)^{2^k} \equiv 1 \quad (2^{k+2}) \qquad \Rightarrow (1+4)^{2^{k-2}} \equiv 1 \ (2^k) \quad k \geq 2$$

et $5^{2^{k-3}} \equiv 1 + 2^{k-1} \ (2^k)$

tout ceci montre que 5 est d'ordre 2^{k-2} mais pas d'ordre 2^{k-3}.

Plus généralement on a :

$$(1+2n)^{2^k} \equiv 1 \ (2^{k+2}) \quad \text{ou} \quad (1+2n)^{2^{k-2}} \equiv 1 \ (2^k) \quad k \geqslant 2$$

$(1+2n)$ représente un nombre impair donc un élément de $(\mathbb{Z}/2^k\mathbb{Z})^*$; on en déduit que tous les éléments de $(\mathbb{Z}/2^k\mathbb{Z})^*$ sont d'ordre 2^{k-2}.

. Exercice : démontrer le théorème suivant :

4.7. Théorème : si n est pair, $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique si et seulement si $n = 2, 4, p^\alpha, 2p^\alpha$, p premier impair.